ელექტრონული მმართველობა და ლიდერობა

ეკატერინე ქარდავა (რედ.)
ზვიად გაბისონია
გიორგი გაბრიელაშვილი
ნიკოლოზ გაგნიძე
გიგა პაიჭაძე
ლევან სამადაშვილი

ელექტრონული მმართველობა და ლიდერობა

თბილისი
2021

მომზადებული და გამოცემულია საჯარო სამსახურის ბიუროს მიერ გაეროს განვითარების პროგრამისა (UNDP) და შვედეთის მთავრობის ხელშეწყობით. გამოთქმული მოსაზრებები ავტორისეულია და შეიძლება არ ასახავდეს დონორი ორგანიზაციების თვალსაზრისს.

წინასიტყვაობა

თანამედროვე საჯარო მმართველობა მუდმივად მზარდი და მრავალფეროვანი გამოწვევების წინაშე დგას. აქტუალურ საკითხთა შორის აღსანიშნავია საჯარო ამოცანების განხორციელება ინოვაციური მმართველობითი მეთოდებით და ინსტრუმენტებით, რაც ელექტრონული მმართველობის შინაარსს ქმნის და თანამედროვე ლიდერებისთვის მძლავრი მმართველობითი იარაღია საჯარო სექტორში არსებული გამოწვევების საპასუხოდ.

ელექტრონული მმართველობა მიზნად ისახავს საჯარო მმართველობის ეფექტურობისა და ეკონომიურობის გაზრდას და სწრაფი, ხარისხიანი და ყოვლისმომცველი სერვისების მიწოდების შესაძლებლობის შექმნას. მისი საშუალებით თანამედროვე ლიდერების ხელში აკუმულირდება დაგეგმვის, ორგანიზების, აღსრულებისა და კონტროლის სწრაფი და ხარისხიანი ინსტრუმენტები. საკითხს აქტუალურობა შემატა მსოფლიოში მიმდინარე პანდემიამ და გამოკვეთა ელექტრონული მმართველობის ღირებულებითი ნაწილი საჯარო მმართველობის შეუფერხებლად განხორციელების უზრუნველსაყოფად.

ამასთან, საჯარო მმართველობის განხორციელება მუდმივად განახლებადი ინოვაციური ტექნოლოგიების გამოყენებით, არსებითად ცვლის სახელმწიფოს მნიშვნელოვანი ფუნქციის – საჯარო მმართველობის – მომავალს, რამდენადაც ზრდადია ტენდენცია მმართველობის პროცესში სულ უფრო ნაკლები ტრადიციული საჯარო-სამართლებრივი ინსტრუმენტის გამოყენების და მათი ჩანაცვლება სამართლებრივად ჯერ კიდევ დაურეგულირებელი, ხელოვნური ინტელექტის გამოყენებით. შესაბამისად, აუცილებელია თანამედროვე ლიდერთა ცნობიერება ამაღლდეს არამხოლოდ ელექტრონული მმართველობის დღეს არსებული ინსტრუმენტების გამოყენების სრულყოფილად ათვისების გზით, არამედ, ასევე გამოიკვეთოს შესაძლო პროგნოზები მომავლის საჯარო მმართველობის დიზაინის თაობაზეც, რათა საჯარო მმართველობის განმახორციელებელი ლიდერები მომზადებული შეხვდნენ მუდმივად განახლებად მმართველობით ინსტრუმენტებს, დააზღვიონ რა საჯარო ინტერესი შესაძლო საფრთხეებისგან და წარმართონ მმართველობითი პროცესი საზოგადოების ინტერესების დაცვისა და ადამიანის უფლებების რეალიზების უზრუნველსაყოფად.

ელექტრონული მმართველობის განვითარება ხასიათდება ორგვარი ეფექტით, კერძოდ მოდერნიზება ყოველთვის დაკავშირებულია პროგრესთან და ამ თვალსაზრისით, დადებითი ზეგავლენის მომტანია საზოგადოებისთვის საჯარო სერვისების ხელმისაწვდომობის, ეკონომიურობისა და ეფექტიანობის პრინციპების ცხოვრებაში გატარების უზრუნველსაყოფად. თუმცა, მმართველობის ინოვაციური მოდერნიზება შესაძლოა უარყოფითი ეფექტის

მომტანიც კი გახდეს, აღნიშნულ პროცესში საჯარო ინტერესის დაცვის საეჭვოობის ირგვლივ არსებული შეკითხვების, ან თუნდაც, ხელოვნური ინტელექტის მეშვეობით მმართველობისას, ადამიანის ღირსების დაცვის, თანაბარი მოპყრობისა და პირადი ცხოვრების ხელშეუხებლობის კონტექსტში არსებული ბუნდოვანების გამო. სამართლებრივი სახელმწიფოს ფუნდამენტური პრინციპებიდან გამომდინარეობს როგორც საჯარო ინტერესის დაცვის, ასევე საზოგადოების თითოეული წევრის უფლებების დაცვის აუცილებლობა. სწორედ ეს მოთხოვნები უნდა იქნეს დაცული საჯარო მმართველობის ინოვაციური ტექნოლოგიების მეშვეობით განხორციელების პროცესში და შესაბამისად, დადგინდეს „მომავლის საჯარო მმართველობის“ იდეური და ფუნქციური შესაბამისობა სამართლებრივი სახელმწიფოს კლასიკურ გაგებასთან. წინამდებარე სახელმძღვანელოს მიზანია განისაზღვროს და დასაბუთდეს საჯარო მმართველობის ინოვაციური მოდერნიზების, ელექტრონული მმართველობის დადებითი ეფექტი საჯარო მმართველობის განხორციელების პროცესში და ხაზი გაესვას შესაძლო საფრთხეებს და მათ პრევენციის აუცილებლობას, რათა სამართალი და სახელმწიფოს მმართველობა ჩიხში არ აღმოჩნდეს და ამით არ დაზიანდეს საჯარო ინტერესი და თითოეული პირის უფლება.

სახელმძღვანელოში განხილულია საკითხები, რაც არსებობს საქართველოში ელექტრონული მმართველობის ირგვლივ და ხაზგასმულია ის გამოწვევები, რაც მომავალში აუცილებლად უნდა იქნეს გადაჭრილი როგორც ქმედითი სამართლებრივი ინსტრუმენტების, ასევე აღსრულების მძლავრი მიდგომების დანერგვის გზით. სახელმძღვანელოში არსებული თემები წარმოადგენს ნებისმიერი საჯარო მოხელის ცნობიერების ამაღლების აუცილებელ ინსტრუმენტს ელექტრონული მმართველობის საკითხებზე და თანამედროვე ლიდერებს აძლევს შესაძლებლობას წინასწარ განჭვრიტონ კარგი მმართველობის უზრუნველსაყოფად საჭირო ღონისძიებები, აიმაღლონ ცოდნა ელექტრონული მმართველობის სიკეთეების და გამოწვევების ირგვლივ.

სარჩევი

ელექტრონული მმართველობის ხელშემწყობი საინტერესო გადაწყვეტები

ელექტრონული პეტიციების პორტალები

პერსონალურ მონაცემთა დაცვა

ელექტრონული მმართველობა – ზოგადი მიმოხილვა

ბოლო რამდენიმე ათეული წელია, ინფორმაციულ-საკომუნიკაციო ტექნოლოგიები (ICT) სწრაფად ვითარდება. დროის გასვლასთან ერთად იზრდება განვითარების ტემპიც, რაც 21-ე საუკუნეში, ციფრული ტრანსფორმაციის ეპოქაში, განსაკუთრებულ როლს თამაშობს არა მხოლოდ ჩვენს ყოველდღიურობაში, არამედ გლობალური დღის წესრიგის ჩამოყალიბებაში, მსოფლიო ეკონომიკაში, საზოგადოების ფორმირებაში, საჯარო ადმინისტრირებასა და მართვაში. ეს მოცემულობა საფუძვლად დაედო ელექტრონული მმართველობის იდეის გაჩენას.

პრაქტიკა გვიჩვენებს, რომ, როგორც წესი, განვითარებადი ქვეყნებისთვის ელმმართველობა განსაკუთრებული ღირებულების მომტანია. თუ შედარებით განვითარებულ ქვეყნებში ინფორმაციულ-საკომუნიკაციო ტექნოლოგიები ხშირად საჯარო სიკეთეებით სარგებლობისთვის დამატებითი, უფრო კომფორტული შესაძლებლობაა, განვითარებადი ქვეყნებისთვის ის ერთ-ერთი ყველაზე ეფექტიანი მექანიზმია კორუფციის შესამცირებლად, საჯარო ფინანსების გამჭვირვალობის უზრუნველსაყოფად, სახელმწიფოს კონტროლისა თუ ანგარიშვალდებულების გასაძლიერებლად და, ჯამში, ეკონომიკური ზრდისა და დემოკრატიული პროცესების განსავითარებლად.[1]

ელექტრონული მმართველობა არ ვითარდება მხოლოდ სახელმწიფოს მხრიდან ქვეყანაში მეტი კომპიუტერის შეძენითა და ვებგვერდის შექმნით, ის, უპირველეს ყოვლისა, არის პროცესი (და არა პროდუქტი), რომელიც მოითხოვს დეტალურ დაგეგმვას, საინფორმაციო-ტექნოლოგიური რესურსების გონივრულად გამოყენებასა და პოლიტიკურ ნებას.

ელექტრონული მმართველობა ტექნოლოგიების გამოყენებით სახელმწიფოსა და მოქალაქის ურთიერთობისთვის ქმნის ახალ, თანამედროვე პლატფორმას, რომლის საშუალებითაც სახელმწიფო სტრუქტურებსა და მოქალაქეებს ერთმანეთთან დაკავშირება შეუძლიათ თანაბარ პირობებში, განურჩევლად მათი ადგილმდებარეობისა. სამთავრობო რესურსების იოლად ხელმისაწვდომობის გზით ელმმართველობა მოქალაქეებისთვის თანაბარი პირობების შექმნას უწყობს ხელს.

ელექტრონული მმართველობის განმარტების მაძიებელი სამეცნიერო ლიტერატურასა[2] და სხვადასხვა საერთაშორისო ორგანიზაციის ვებსაიტზე[3] უამრავ განსხვავებულ ვერსიას შეხვდება. არსებობს განსხვავებული თეორიები და მათი პრაქტიკული რეალიზების მაგალითებიც მრავალფეროვანია. ელექტრონული მმართველობის არსის განმარტებისთვის მნიშ-

---

1 ვალენტინა (დარდა) ნდოუ – „ელმმართველობა განვითარებად ქვეყნებში – შესაძლებლობები და გამოწვევები“. წყარო: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.127.9483&rep=rep1&type=pdf

2 Shailendra C. Jain Palvia and Sushil S. Sharma (2007). “E-Government and E-Governance: Definitions/Domain Framework and Status around the World“

3 გაეროს ელმმართველობის უნივერსიტეტი – https://egov.unu.edu; ევროპული კომისია: https://ec.europa.eu/info/business-economy-euro/egovernment_en; ევროპის საბჭო: https://www.coe.int/t/dgap/democracy/Activities/GGIS/E-governance/Default_en.asp

ვნელოვანია სხვა ისეთ სიტყვათშეთანხმებებსაც შევეხოთ, როგორებიცაა ელექტრონული მთავრობა და ელექტრონული დემოკრატია.

ზოგჯერ „ელმმართველობისა“ და „ელექტრონული მთავრობის“ ცნებებს შეცდომით სინონიმებად იყენებენ, თუმცა მიზანშეწონილია მათი გამიჯვნა: ელექტრონული მმართველობა (e-governance) უფრო ფართო ცნებაა, ვიდრე ელექტრონული მთავრობა (e-government), ვინაიდან ის გულისხმობს მოქალაქესა და საჯარო სექტორს შორის ურთიერთობის ცვლილებებსაც.[4] ელექტრონული მმართველობა გვთავაზობს ახალ კონცეფციებს მოქალაქის როლთან, მის საჭიროებებთან და უფლებამოსილებებთან დაკავშირებით. ელექტრონული მმართველობის მთავარი დანიშნულებაა მოქალაქის როლისა და უნარების გაძლიერება, მისი უფლებების დაცვის, რეალიზების ხარისხისა და საჯარო სექტორის საქმიანობაში მისი ჩართულობის გაზრდა.

ელექტრონული მმართველობა არის ინფორმაციულ-საკომუნიკაციო ტექნოლოგიებზე დაფუძნებული კონცეფცია დემოკრატიული პროცესების გასაძლიერებლად და განვითარების ხელშესაწყობად. ის უზრუნველყოფს საზოგადოებრივ-სოციალურ ცვლილებებზე მთავრობის უკუკავშირის, საპასუხო ქმედებების გაძლიერებას. ელექტრონული მმართველობის მთავარი დანიშნულებაა მთავრობის ოპერაციული ეფექტიანობის გაძლიერება და მოქალაქეთა მოთხოვნების უკეთ დაკმაყოფილება უფრო გაუმჯობესებული საჯარო მომსახურების მიწოდებით. ერთ-ერთი შეფასებით, ელექტრონული მმართველობა უფრო მეტად უკავშირდება ქვეყანაში დემოკრატიულ პროცესებს, ვიდრე ადმინისტრაციულ რეფორმებს.[5]

ზოგადად, ელექტრონული მმართველობა არის სახელმწიფოს ნება, გამოიყენოს თანამედროვე ინფორმაციულ-საკომუნიკაციო საშუალებები, რათა თავად მთავრობა და მისგან მიწოდებული მომსახურება გახადოს უფრო ეფექტიანი, მოქნილი და ადვილად ხელმისაწვდომი. ელექტრონული მმართველობა მოიცავს:

- სამთავრობო ინფორმაციის მარტივად ხელმისაწვდომობას;
- მოქალაქეების ჩართულობას საჯარო მოსამსახურეებთან უშუალო კომუნიკაციის გზით;
- მთავრობის ინფორმაციულ ღიაობას მისი საქმიანობის მაქსიმალურად გამჭვირვალედ წარმოჩენის გზით;
- ინტერაქტიურობას, რაც ხსნის საზღვრებს სხვადასხვა ქალაქისა და სოფლის მოსახლეობისთვის და აძლევს მათ თანაბარ შესაძლებლობას, ონლაინ რეჟიმში მიიღონ სამთავრობო მომსახურებები, რაც ზოგავს მათ დროსა და ფინანსებს.

---

4 ჰერმან სინი – „რა განსხვავებაა ელმმართველობასა და ელმთავრობას შორის?“. წყარო: https://www.jagranjosh.com/general-knowledge/what-is-the-difference-between-egovernment-and-egovernance-1503018565-1

5 Toni G.L.A. van der Meer, Dave Gelders and Sabine Rotthier, *e-Democracy: Exploring the Current Stage of e-Government,* Journal of Information Policy, Vol. 4, 2014.

ელექტრონული მთავრობა ასოცირდება ინფორმაციულ-საკომუნიკაციო ტექნოლოგიების გამოყენებასთან, თუმცა მთავარი აქცენტი აღნიშნულ ტექნოლოგიებზე არ კეთდება. ელ-მთავრობის მთავარი განმაპირობებელია ორგანიზაციულ-ინსტიტუციური ცვლილებები და ახალი უნარ-ჩვევების დამკვიდრება საჯარო სექტორში, რაც იწვევს საჯარო მომსახურების, დემოკრატიული პროცესებისა და საჯარო პოლიტიკის გაუმჯობესებას.

ძირითადად, ელექტრონული მთავრობა ორი მთავარი კომპონენტისგან შედგება: საჯარო მომსახურების მიწოდება საზოგადოებისთვის – **ელმომსახურება** და მთავრობის საჯარო მმართველობის პროცესების გაუმჯობესება – **ელადმინისტრირება**. სწორედ ამ ორი მი-მართულების განვითარება მოიაზრება ელმთავრობის განხორციელებისას.

საკითხის არსის უკეთ გასაგებად, განვიხილოთ ელექტრონული დემოკრატიისა და მასთან მჭიდროდ დაკავშირებული ელექტრონული მონაწილეობისა და ჩართულობის საკითხე-ბიც. ელექტრონული დემოკრატია ელექტრონული მმართველობის განვითარების განუ-ყოფელი ნაწილია. ელექტრონული დემოკრატია ნიშნავს ტექნოლოგიური საშუალებების გონივრულად გამოყენებას არსებული ელექტრონული მმართველობის მოდელებისა და პრაქტიკის გამდიდრებისა თუ გარდაქმნისათვის. აღნიშნული ტექნოლოგიები მნიშვნე-ლოვნად ზრდის მთავრობის გამჭვირვალობას, პასუხისმგებლობას და ანგარიშვალდებუ-ლებას, სთავაზობს რა მოქალაქეებს დამატებით შესაძლებლობას, მონაწილეობა მიიღონ პოლიტიკურ პროცესებში, შედეგად კი ვიღებთ მთელი საზოგადოებისთვის უკეთეს პოლი-ტიკურ გადაწყვეტილებებს.

ელექტრონული დემოკრატია მოიცავს საზოგადოების ყველანაირი ელექტრონული ფორ-მით, პროცესითა და წესით ინტერაქციას მთავრობასთან და არჩეულ წარმომადგენლებ-თან. ელექტრონულ დემოკრატიაში მოიაზრება ინფორმაციულ-საკომუნიკაციო ტექნოლო-გიების გამოყენება საჯარო პოლიტიკის პროცესებში მოქალაქეთა მონაწილეობის, მათი ჩართულობის უზრუნველსაყოფად.

ელექტრონული დემოკრატიის მხარდასაჭერად, ტექნოლოგიები გამოიყენება ინფორმა-ციის გასაჯაროებისათვის, მისი მიწოდების გასაუმჯობესებლად, მოქალაქეთა აქტიური მო-ნაწილეობისა და კონსულტაციის პროცესის წარსამართად. ელექტრონულ დემოკრატიაში ინფორმაციას, კონსულტაციებსა და მონაწილეობას გადამწყვეტი მნიშვნელობა ენიჭებო-და თავდაპირველ ეტაპზე – ტიპური „top-down“ მიდგომა ელექტრონულ დემოკრატიაში, – მომხმარებლების ინფორმაციაზე წვდომისა და მთავრობის მიერ ინიცირებულ პროცესებზე რეაგირების შესაძლებლობებით. „Top-down“ მიდგომა შემდგომ, საზოგადოების უფრო აქ-ტიური ჩართულობის შედეგად ტრანსფორმირდა და მივიღეთ „bottom-up“ პროცესი.[6] აღ-ნიშნული მიდგომის შესაბამისად, მოქალაქეები საჯარო სექტორის მომსახურების პასიური

[6] Niels Jørgensen – Design in e-Government Curricula: Bottom-Up vs. Top-Down. წყარო: https://www.researchgate.net/publication/228635038_Design_in_e-Government_Curricula_Bottom-Up_vs_Top-Down

მომხმარებლებიდან საჯარო პოლიტიკის შემქმნელებად იქცევიან. მაგ., მთავრობის მიერ შედგენილ სამოქმედო გეგმაზე პასიური რეაგირების ნაცვლად, მოქალაქეები თავად განსაზღვრავენ სამთავრობო გეგმებსა და პრიორიტეტებს მთავრობისთვის. შედეგად, ქვეყნის განვითარების კურსის განსაზღვრის მიმართულებით მოქალაქეთა შესაძლებლობები ძლიერდება და ამ პროცესში საზოგადოების მონაწილეობა სულ უფრო მნიშვნელოვანი ხდება.

ელმმართველობის განვითარების პროცესი შესაძლოა განსხვავებულად მიმდინარეობდეს სხვადასხვა ქვეყანაში, თუმცა აღსანიშნავია შემდეგი ძირითადი პრინციპები და ტენდენციები:

მომხმარებლებზე, მოქალაქეზე ორიენტირებულობა (Citizen First/Citizen Centricity)

ტექნოლოგიებით მხარდაჭერილი სერვისები ინდივიდზე უნდა იყოს ორიენტირებული. „მოქალაქეები საჯარო სამსახურის ცენტრში“ – ეს კონცეფცია უნდა მუშაობდეს ადმინისტრაციულ ორგანოებში, როგორც კარგი, დემოკრატიული მმართველობის ერთ-ერთი პრინციპი. მოქალაქისათვის 24/7 ხელმისაწვდომი უნდა იყოს ყველა ელექტრონული სერვისით დატვირთული ერთიანი პორტალი. ასეთი კონცეფცია მოქალაქეებს ეხმარება იმის სრულფასოვნად გაცნობიერებაში, თუ რომელ ელექტრონულ სერვისებს სთავაზობს სახელმწიფო და ხელს უწყობს ამ სერვისების ფართომასშტაბიან გამოყენებას.

„მხოლოდ ერთხელ“ (Once only). მოქალაქეები და იურიდიული პირები საჯარო დაწესებულებას მხოლოდ ერთხელ წარუდგენენ თავიანთ მონაცემებს. პერსონალურ მონაცემთა დაცვისა და პირადი ცხოვრების ხელშეუხებლობის პრინციპების გათვალისწინებით, ინფორმაციის საჭიროების შემთხვევაში, საჯარო დაწესებულებები ერთმანეთს უცვლიან მონაცემებს, შესაბამისად, მოქალაქეებს/იურიდიულ პირებს აღარ მოეთხოვებათ საჯარო დაწესებულებისათვის ინფორმაციის განმეორებით წარდგენა.

მოქალაქეებს, რომლებიც ადმინისტრაციულ ორგანოებს ყოველ ჯერზე ახალი მომსახურების მისაღებად მიმართავენ, აღარ მოეთხოვებათ ინფორმაციის განმეორებით წარდგენა საჯარო დაწესებულებისთვის. ამის ნაცვლად, ერთხელ მიწოდებული მონაცემები ინახება შესაბამის ბაზაში და მონაცემთა უსაფრთხო გაცვლის პლატფორმის საშუალებით ინფორმაცია ერთი ადმინისტრაციული ორგანოდან გადაეგზავნება მომთხოვნ დაწესებულებას. ამ პრინციპის ფართომასშტაბიანი დანერგვით, მოქალაქეების ადმინისტრაციული ტვირთის შემცირებასთან ერთად იზრდება მათ მიერ პერსონალურ მონაცემებზე კონტროლის შესაძლებლობაც და ეს ასევე ეხმარება საჯარო დაწესებულებებს უფრო სწრაფად, გამჭვირვალედ და ეფექტიანად მუშაობაში.

„ერთი სარკმლის“ პრინციპი – ერთიანი საკონტაქტო არხი (Single Points of Contact)

ერთი სარკმლის პრინციპი უზრუნველყოფს ინფორმაციისა და სახელმწიფო ორგანოების სერვისების წვდომას საერთო პლატფორმაზე, მომხმარებლის უცვლელი ინტერფეისით. ეს საშუალებას აძლევს მომხმარებელს, ადგილმდებარეობის მიუხედავად ისარგებლოს პროდუქტებისა და სხვადასხვა საჯარო უწყებების სერვისების ფართო სპექტრით, ცენტრალური წვდომის საშუალებით.

შესაბამისად, ყველა მოქალაქეს შეუძლია, მაგალითად, ერთ ადგილზე მოიძიოს შესაბამისი ინფორმაცია, საჯარო დაწესებულების საკონტაქტო მონაცემები, განცხადებების/საჩივრების ფორმები და ა.შ. ეს ზრდის სერვისზე ორიენტაციას და ზოგავს მომხმარებლის დროს და დანახარჯებს ტრანზაქციის დამუშავებისას.

ერთიანი საკონტაქტო წერტილი (PSCs) ეწოდება ელმმართველობის ონლაინ პორტალებს, რომლებიც საშუალებას აძლევს სერვისით დაინტერესებულ პირებს, მიიღონ საჭირო ინფორმაცია და ონლაინ შეასრულონ ადმინისტრაციული პროცედურები ერთ პორტალზე, ერთი საკონტაქტო რგოლის მეშვეობით.

„უწინარეს ციფრულად“ (Digital First). „უწინარეს ციფრულად“ სოციალურ-ეკონომიკური ზრდის გარანტიაა, რადგან ის ბიზნესსექტორში ახალი უნარების შეძენას და, ზოგადად, მოქალაქეებში ციფრული კულტურის განვითარებას უწყობს ხელს, რაც ჯამში გამოიწვევს მათი კონკურენტუნარიანობის ზრდას საერთაშორისო ბაზარზე, ციფრულ პროდუქტებზე გაზრდილი მოთხოვნა კი შესაძლოა, ინოვაციების საფუძველი გახდეს.

„უპირობოდ ციფრული“ (Digital by default). თითოეული სახელმწიფო უწყება ვალდებულია, ყოველი ახალი მომსახურების შექმნისას ალტერნატივის სახით უზრუნველყოს ციფრული მომსახურების არსებობა, ხოლო უკვე არსებული მომსახურება ხელმისაწვდომი გახადოს ციფრულ ფორმატშიც. მოქალაქეებისთვის ყველა სერვისი ხელმისაწვდომი უნდა იყოს ელექტრონულად. თუ მხოლოდ ზოგიერთ მომსახურებას ვაციფრულებთ, სხვებს კი – არა, ეს გამოიწვევს მომხმარებლების იმედგაცრუებას და შეამცირებს საჯარო სისტემისადმი ნდობას. შემოთავაზებული სერვისები უნდა იყოს სრული და სრულყოფილი, მომხმარებელს მომსახურების მიღების პროცესის დასრულების მიზნით ოფისში მისვლა არ უნდა სჭირდებოდეს.

ელმმართველობა ხელს უწყობს მთავრობის ანგარიშვალდებულებას, გამჭვირვალობას, ღიაობასა და საზოგადოების ინტერესებზე ორიენტირებული საჯარო პოლიტიკის განხორციელებას. მას განვითარებად, გარდამავალი დემოკრატიული პროცესების მქონე ქვეყნებში დადებითი ანტიკორუფციული გავლენა აქვს, აგრეთვე საგრძნობლად ამცირებს ადმინისტრაციულ ტვირთს საზოგადოებისა და ბიზნესისთვის. აქვე მნიშვნელოვანია აღინიშნოს, რომ ელმმართველობა თავად ვერ იქნება რეფორმების განხორციელების მამოძრავებელი ძალა, თუმცა იგი რეფორმების მხარდამჭერ მნიშვნელოვან იარაღად შეიძლება აღვიქვათ.

ელმმართველობა მთავრობის ტრანსფორმაციისა და ქვეყნის დემოკრატიული განვითარების პროცესში „ყოვლისშემძლე“ იარაღი არ არის.[7] სოციალური, პოლიტიკური, ეკონომიკური და კულტურული ფაქტორები ძალზე მნიშვნელოვან როლს თამაშობს, თუმცა ადგილობრივ რეალობაზე მორგებული ელმმართველობის სტრატეგიული დანერგვით ქვეყნებს წარმატებული და ეფექტური რეფორმების განხორციელების შესაძლებლობა ეძლევათ.

[7] შეად.: Kate OAKLEY „What is e-governance?“, წყარო: https://www.coe.int/t/dgap/democracy/activities/ggis/e-governance/Work_of_egovernance_Committee/Kate_Oakley_eGovernance_en.asp

ლიდერობა და მართვა ციფრულ სამყაროში

რა არის ლიდერობა

ლიდერობის ერთი, უნივერსალური განმარტება არ არსებობს და ლიტერატურაში სხვადასხვაგვარად აღწერენ. თუმცა ყველა ვთანხმდებით, რომ ლიდერობა, უპირველეს ყოვლისა, დაკავშირებულია გავლენის უნართან და არა კონკრეტულ პოზიციასთან ან თანამდებობასთან, როგორც ხშირად წარმოგვიდგენია. ცხადია, შესაძლოა მაღალი პოზიცია მნიშვნელოვანი ხელშემწყობი ფაქტორი იყოს, მაგრამ ეს საკმარისი არ არის, რომ ადამიანები პატივს გვცემდნენ, გვენდობოდნენ, საქმეში მოგვყვებოდნენ და გვიჯერებდნენ. ამისათვის კი პოზიციაზე გაცილებით მნიშვნელოვანი ლიდერული ქცევაა. შესაბამისად, ნებისმიერ პოზიციაზე მდგომ ადამიანს შეუძლია გახდეს ლიდერი, თუ მას აქვს უნარი, საკუთარი ქცევით მოახდინოს გავლენა ორგანიზაციაში მომუშავე ადამიანებზე.

როგორ არჩევენ სპორტულ გუნდებში კაპიტანს? კაპიტნები ხშირად გუნდში ყველაზე სწრაფი, ძლიერი, ტექნიკური ან განსაკუთრებული სპორტული უნარებით დაჯილდოებული ადამიანები სულაც არ არიან. თუმცა, რაც მათ ნამდვილად გამოარჩევთ, ეს ისევ და ისევ ლიდერული ქცევაა, რომელიც გავლენას ახდენს გუნდის ყველა წევრზე.

რა ტიპის ქცევაზე ვსაუბრობთ? კაპიტნები მუდმივ კონტაქტში არიან სხვა წევრებთან, აძლევენ უკუკავშირს, ინტერესდებიან მათი სამუშაოს შესრულების ხარისხით, პრობლემებით, მზად არიან, დაეხმარონ, მისცენ რჩევა, აკვირდებიან ფართო სურათს და ყურადღება მხოლოდ საკუთარ თავზე, საკუთარ პასუხისმგებლობებზე არ აქვთ მიმართული; გამოდიან ინიციატივებით, არ უარობენ მეტი პასუხისმგებლობის აღებას და, საჭიროების შემთხვევაში, ისეთი საქმის გაკეთებას, რომელიც შეიძლება უშუალოდ მათ მოვალეობებში პირდაპირ არც იყოს განსაზღვრული. ცხადია, ეს არ ნიშნავს უხეშ ჩარევას სხვის პასუხისმგებლობებში ან თანამშრომლებისთვის უსარგებლო აქტიურობით თავის მობეზრებას, თუმცა ორგანიზაციებში ყოველთვის არის ადგილი საკუთარ სფეროში ლიდერობისთვის, ისე რომ უხეშად არ შევიჭრათ სხვის კომპეტენციებში. ლიდერული უნარ-ჩვევები იმასაც გულისხმობს, რომ სწორად განვსაზღვროთ ჩვენი სამოქმედო არეალი და საკუთარ ქმედებებთან დაკავშირებული შესაძლო სასარგებლო შედეგები.

აღსანიშნავია, რომ ლიდერის სტატუსს ამგვარი ადამიანები არა კაპიტნად დანიშვნის შემდეგ მოიპოვებენ, არამედ პირიქით – უკვე ლიდერად ჩამოყალიბებულ ადამიანებს შეარჩევენ ხოლმე ასეთ პოზიციაზე.

ეს მსჯელობა რომ საჯარო სამსახურის მაგალითზე გადმოვიტანოთ – ლიდერივით მოქცევა ნებისმიერ პოზიციაზეა შესაძლებელი და ამისთვის აუცილებელი არ არის მაღალი თანამდებობა. უპირველესად, უნდა ვეცადოთ, ჯერ ლიდერებად ჩამოვყალიბდეთ და მხოლოდ ამის შემდეგ მოვხვდეთ ხელმძღვანელ პოზიციებზე. ამას დიდი მნიშვნელობა აქვს სხვადასხვა პრაქტიკული გამოწვევის დასაძლევად. კერძოდ, ადამიანებთან, რომლებიც მაღალ პოზიციებზე ხვდებიან და თანამშრომლები მათ ლიდერებად არ აღიქვამენ, ვაწყ-

დებით ე.წ. აღიარების პრობლემას – მიუხედავად პოზიციისა, თანამშრომლებს ნაკლებად სურთ, მიჰყვნენ ხელმძღვანელ პირს, რადგან არ აქვთ მისი საკმარისი ნდობა, პატივისცემა და სხვა მნიშვნელოვანი ფაქტორები. ასეთ შემთხვევებში ხელმძღვანელ პირს განსაკუთრებული ძალისხმევა სჭირდება. ის არ უნდა ფიქრობდეს, რომ, რადგან უფროსია, თანამდებობრივად უფრო მაღალ იერარქიულ საფეხურზე, მის ნებისმიერ დირექტივას გარანტირებულად დაემორჩილებიან. განწყობა – „დირექტორი მე ვარ და გადაწყვეტილებებსაც მე ვიღებ“ – ხანგრძლივ პერსპექტივაში ვერასდროს იქნება ორგანიზაციის ეფექტიანობის განმსაზღვრელი და აუცილებლად წარუმატებლად დასრულდება. შესაბამისად, ამ განწყობას მუდმივი იმედგაცრუება მოჰყვება, თუ თანამშრომლები ლიდერად არ გვაღიარებენ და მათზე გავლენას ვერ ვახდენთ, უპირველეს ყოვლისა, ჩვენი ქცევით, ჩვენი მაგალითიდან გამომდინარე.

სიტუაცია კიდევ უფრო რთულია ისეთ შემთხვევებში, როდესაც გუნდის შიგნიდან აწინაურებენ ვინმეს. ამ შემთხვევაში თანამშრომლები უკვე იცნობენ ახლად დანიშნულ ხელმძღვანელს, მის შესახებ უკვე გააჩნიათ აზრი და შთაბეჭდილება. თუ ამ ადამიანს უკვე ლიდერად არ მიიჩნევენ, მაშინ კიდევ უფრო ნაკლები ენთუზიაზმით მოეკიდებიან მისი იდეების, მიზნების, მითითებების განხორციელებას. ხშირ შემთხვევაში, შესაძლოა ამას დაერთოს კონკურენციის ფაქტორიც და მიზანმიმართული ქმედებები ლიდერის დისკრედიტაციის მიზნით, რაც, სამწუხაროდ, არცთუ იშვიათია. აქედან გამომდინარე, ახლად დაწინაურებულ ხელმძღვანელს განსაკუთრებული ძალისხმევა, სიფრთხილე და ყურადღება მართებს თანამშრომლებში ლიდერის სტატუსის მოსაპოვებლად, რისთვისაც მხოლოდ მისი ახალი თანამდებობა საკმარისი არ იქნება.

დასასრულ, ხაზგასმით აღსანიშნავია, რომ აუცილებელია, ჩვენი ცოდნით, შრომით განვითაროთ შესაბამისი უნარები და ჩვენი მოქმედებები სულ უფრო მეტად დაემსგავსოს ლიდერის ქცევას. ამისთვის აუცილებელი არ არის, „დაბადებით ლიდერები“ ვიყოთ, როგორც, შესაძლოა, ხანდახან გაგვიგია. გაცილებით მნიშვნელოვანია გააზრებული და მიზანმიმართული მუშაობა საკუთარ თავზე, რომ ორგანიზაციისთვის მნიშვნელოვანი, ეფექტიანი თანამშრომლები გავხდეთ.

ლიდერების დამახასიათებელი მიდგომები და დამოკიდებულებები

ლიდერული უნარ-ჩვევების გამომუშავების გზაზე შესაბამისი დამოკიდებულებებისა და მიდგომების განვითარებას განსაკუთრებულ მნიშვნელობა აქვს. მნიშვნელოვანია გავაცნობიეროთ, რა ტიპის თანამშრომლები გვყავს ორგანიზაციაში ან რა მიდგომების მქონე თანამშრომლები ვართ ჩვენ თვითონ:

გამცემი თუ მომხმარებელი? ხშირად სამსახურში თანამშრომელთა უმეტესობა ორიენტირებულია მიღებაზე ან „წამოღებაზე“. ჩვეულებრივ, ეს შეიძლება იყოს უბრალოდ ფინანსური სარგებელი ხელფასის, ბონუსის, ჯანმრთელობის დაზღვევისა და სხვა სარგებლის სახით. ხშირად ეს არის სტატუსი, ასევე, გამოცდილება, კვალიფიკაცია, ინფორმაცია. ცხადია, ამ მოტივაციის, ამ საკითხების განხილვის გარეშე სამსახურის დაწყების გადაწყვეტილებას არავინ იღებს. თუმცა ლიდერი იმასაც შეეცდება, რომ გააცნობიეროს, თავად რას შესთავაზებს ორგანიზაციას ან მთლიანად საჯარო სამსახურს.

ალბათ ბევრს გაუჩნდება კითხვა: რა შემიძლია შევთავაზო ან რას ვფლობ განსაკუთრებულს? სინამდვილეში, აუცილებელი არაა, ამ კონტექსტში მხოლოდ რევოლუციური ცვლილებები და მასშტაბური ინოვაციები განვიხილოთ. რის შეთავაზებაც ყველას შეგვიძლია, არის თუნდაც იმაზე ოდნავ მეტი, ვიდრე ფორმალურად გვევალება. ვიმუშაოთ სხვებზე მეტი, ხშირად გამოვიჩინოთ ინიციატივა, უფრო აქტიურად ვიყოთ ჩართულები ორგანიზაციის ცხოვრებაში და არ ჩამოვიყალიბოთ მუდმივი მომხმარებლის ფსიქოლოგია. მთავარი გარდატეხა ჩვენს გონებაში უნდა მოხდეს და თუ ჩვენს შესაძლებლობებს ვირწმუნებთ, აუცილებლად მოვახერხებთ, მომხმარებელთან ერთად, მნიშვნელოვანი სარგებლის გამცემები ვიყოთ.

ცვლილება თუ სტატუს კვო? უკეთეს გარემოში, ორგანიზაციაში ყოფნა ალბათ ნებისმიერს სურს. ამისთვის ყველას შეგვიძლია, თუნდაც მინიმალური გავიღოთ და პოზიტიურ ცვლილებას შევუწყოთ ხელი. ამის ერთ-ერთი გზა ზემოთ აღწერილი, „მომხმარებლის“ დამოკიდებულების „გამცემით“ შეცვლაცაა. გარდა ამისა, შეგვიძლია დავკავდეთ pro bono[8], სამოხალისეო საქმით, ხელი შევუწყოთ მნიშვნელოვანი პროექტების განხორციელებას მათი მხარდაჭერით, რაც შეიძლება თუნდაც ამ ინიციატივების შესახებ ინფორმაციის გაზიარებაში, ცნობილობასა და კომუნიკაციაში დახმარებით გამოიხატოს, სულ მცირე, ჩვენსავე სამეგობრო წრეში. ისევ და ისევ, მთავარია, გვჯეროდეს და ვაცნობიერებდეთ, რომ უკეთესობისკენ ცვლილებისთვის თუნდაც მცირეს გაღება ყველას შეგვიძლია.

მგრძნობიარობა. ლიდერული დამოკიდებულება იმ საკითხებისადმი, გამოწვევებისადმი სენსიტიურობასაც გულისხმობს, რომლებიც სხვებზე ახდენენ გავლენას. ბუნებრივი და არა ყალბი ემპათია ლიდერის ერთ-ერთი მნიშვნელოვანი თვისებაა. თუ საკითხს ასე არ ვუდგებით, არ ვგულშემატკივრობთ ცვლილებას, კონკრეტული ჯგუფების ან საზოგადოებისთვის რაიმეს გაუმჯობესებას, დიდი ალბათობაა, რომ ავირჩევთ მომხმარებლის, სტატუს კვოს, „სულ ერთიას“ გზას. ხშირად ეს გზა, იმედგაცრუების შედეგია, თუმცა, ლიდერს ის თვისებაც განასხვავებს, რომ იოლად არ ეგუება გარემოს, ზოგჯერ თავსმოხვეულ ან საზოგადო უიმედობის განცდას.

ქმედება. მიუხედავად იმისა, რომ ქმედება შესაძლოა თავისთავად, ბუნებრივ ძალისხმევად მიგვაჩნდეს, ყოველთვის ასე არ არის. ზემო ხსენებული სამი ფაქტორის არსებობის შემთხვევაშიც კი შეიძლება გაჩნდეს მნიშვნელოვანი ბარიერები, როგორებიცაა: ნიჰილიზმი, უნდობლობა, ორგანიზაციაში არსებული არასწორი სტიმულები და ა.შ. ლიდერი მარტივად არ ეგუება ბარიერებს, იმის ნაცვლად, რომ საკუთარი უმოქმედობა და მომხმარებლური დამოკიდებულება გარე ფაქტორების, გარე ბარიერების არსებობით გაამართლოს, ის ეძებს გზებს, ქმედებებსა და საშუალებებს, როგორ მოიტანოს სარგებელი ორგანიზაციული, საჯარო, და საუკეთესო საზოგადო ინტერესისთვის.

[8] საზოგადოებრივი სიკეთისკენ მიმართული.

ლიდერული უნარ-ჩვევები არ არის თანდაყოლილი და სურვილის შემთხვევაში მათი გამომუშავება შეიძლება. ამაზე ზრუნვა არა მხოლოდ ჩვენი, როგორც პროფესიონალების, ინდივიდუალური პასუხისმგებლობაა, არამედ ორგანიზაციის ამოცანაც. ორგანიზაცია უნდა აცნობიერებდეს თავის ეფექტიანობასა და თანამშრომელთა ლიდერულ უნარებს შორის არსებულ მყარ კავშირს. ლიდერული თვისებები, როგორებიცაა გადაწყვეტილების მიღების უნარი, მოქნილობა, გარემოსთან სწრაფად ადაპტაცია, კარგი კომუნიკაცია, კოლეგების მოტივაციის უნარი და ასე შემდეგ, ყველა თანამშრომლისთვის თანაბრად მნიშვნელოვანია როგორც პიროვნული, პროფესიული წარმატებისთვის, ასევე, ჯამში, ორგანიზაციული ეფექტიანობისთვის. ორგანიზაციები განსაკუთრებულ წარმატებას მხოლოდ მაშინ აღწევენ, როდესაც ლიდერულ თვისებებს მაქსიმალურად ბევრი თანამშრომელი ავლენს.

იმისთვის, რომ ორგანიზაციაში გვქონდეს ლიდერული უნარ-ჩვევებისა და თვისებების განვითარების მოტივაცია, შესაბამისი ორგანიზაციული კულტურის და სტიმულების არსებობაა აუცილებელი. ორგანიზაციული კულტურის განვითარებასა და შენარჩუნებაზე კი განსაკუთრებული პასუხისმგებლობა იერარქიის მაღალ საფეხურზე მყოფ ადამიანებს – ორგანიზაციის ხელმძღვანელ პირებს ენიჭებათ.

ლიდერები და მენეჯერები

ლიდერებს და მენეჯერებს ბევრი თვისება აერთიანებთ და შესაბამისად, ხშირად, სინონიმებად ვიყენებთ. მიუხედავად ამისა, არის მნიშვნელოვანი განსხვავებებიც. მენეჯერები მეტწილად მიმართულნი არიან მოკლევადიან მიზნებზე და მათ განხორციელებაზე, პროცესების მართვასა და მათ გაუმჯობესებაზე, ყოველდღიურ მენეჯმენტზე. ძალაუფლების ძირითადი წყარო მათი პოზიციაა, რომლის შესაბამისადაც ხელმძღვანელობენ დაქვემდებარებულ სტრუქტურულ ერთეულებს. ლიდერები კი თავად აყალიბებენ ხედვასა და მიზნებს, შესაბამისად, უფრო ხანგრძლივ პერიოდზე აქვთ ფოკუსი. ლიდერები თანამშრომლებს შთააგონებენ, უღვიძებენ მოტივაციას, მათი ძალაუფლების ძირითადი წყარო კი არის გავლენა ადამიანებზე, რომელთაც საკუთარი ქცევით და მაგალითის მიცემით მოიპოვებენ. ლიდერებს, ასევე, აქვთ განსაკუთრებული როლი, ხელი შეუწყონ ორგანიზაციის ძირითადი ფუნქციური მიმართულებების კოორდინაციას და ინტეგრაციას, მათ შორის – ადამიანური რესურსების, საინფორმაციო ტექნოლოგიების, კომუნიკაციისა და მარკეტინგის, ფინანსებისა და სხვა კრიტიკული სფეროების ჰარმონიულ მუშაობას. ამასთან, ლიდერმა უნდა უზრუნველყოს, რომ სხვადასხვა დეპარტამენტის საქმიანობა მყარად უკავშირდებოდეს ორგანიზაციის ფართო მიზნებს და ორგანიზაციული ხედვა განხორციელდეს ოპტიმალური გზებით.

ზემოაღწერილი განსხვავებების მიუხედავად, ისევე როგორც მენეჯერისთვის, ლიდერისთვისაც აუცილებელია მართვის კარგი უნარების განვითარება, რადგან ის ჩართულია მენეჯ-

მენტის ოთხი ძირითადი ფუნქციის განხორციელებაში: დაგეგმვა; ორგანიზება; გაძღოლა; კონტროლი.

ლიდერებმა განსაკუთრებული ყურადღება უნდა მიაქციონ, თუ რამდენ დროს უთმობენ თითოეულ ფუნქციას, რადგან მათ შორის შესაბამისი ბალანსის არსებობა მნიშვნელოვანია. ხშირად ადამიანები მეტ დროს უთმობენ იმ საკითხებს, რომლებიც უფრო მეტად სიამოვნებთ, ეხერხებათ, უიოლდებათ და ასე შემდეგ. ასეთ შემთხვევაში, მცირდება სხვა მნიშვნელოვანი ფუნქციების ეფექტიანად განხორციელების ალბათობა და, შესაბამისად, იზრდება წარუმატებლობის რისკიც.

ლიდერები წარმატებით ახერხებენ, გადაწყვიტონ მართვასთან დაკავშირებული შემდეგი მნიშვნელოვანი გამოწვევები:

ბალანსი მიზნის სიცხადესა და დისკრეციას შორის – მიზნის სიცხადე და დისკრეციის დონე მნიშვნელოვნად განსაზღვრავს ორგანიზაციაში არსებულ სტიმულებს, ორგანიზაციულ გარემოსა და კულტურას. რაც უფრო მეტია დისკრეცია, მიზანი კი – ნათელი, თანამშრომლები მეტი მოტივაციით მიდიან მიზნისკენ; მაღალი დისკრეციისა და ბუნდოვანი მიზნის თანხვედრისას ხშირია დაბნეულობა და ფრუსტრაცია; დაბალი დისკრეცია და ნათელი მიზანი დავალებების მინიმალურ, მაღალი მოტივაციის გარეშე შესრულებას განაპირობებს, ხოლო დაბალი დისკრეცია და ბუნდოვანი მიზანი – სრულიად უინტერესო, უმოტივაციო სამუშაო პროცესს.

ორგანიზაციული სტრესის ბალანსი – ლიდერმა უნდა უზრუნველყოს, რომ ორგანიზაციული სტრესის დონე თანამშრომლის ოპტიმალურ ჩართულობას განაპირობებდეს. ხშირად, ზედმეტად ბევრი თანამშრომელი და ცოტა საქმე პროდუქტიულობას ამცირებს და მოტივაციაზეც უარყოფითად აისახება. სტრესის გამომწვევად შესაძლოა ასევე იქცეს მონიტორინგის სუსტი სისტემა ან ამ უკანასკნელის არარსებობა. ცხადია, სტრესი არასასურველია, რაც ხანგრძლივ პერსპექტივაში ხშირ შეცდომებს, თანამშრომელთა „გადაწვას“ და ეფექტიანობის შემცირებას იწვევს.

მხარდაჭერის განცდის უზრუნველყოფა – ლიდერს განსაკუთრებული როლი აკისრია მიმდევრების მხარდაჭერის, მათი მოტივირების მხრივ. ამასთან, მის მიმდევრებს არ უნდა ეშინოდეთ წარუმატებლობის, უნდა ჰქონდეთ სტიმული ახალი იდეების, სარისკო და საპასუხისმგებლო გადაწყვეტილებების მისაღებად. აუცილებელია, ლიდერის მხრიდან პასუხისმგებლობის გაზიარება არა მხოლოდ წარმატებისას, არამედ წარუმატებლობისასაც. მხარდაჭერის განცდის დასანერგად ასევე აუცილებელია გადაწყვეტილების მიღების პროცესში ერთობლივი მონაწილეობის განცდის უზრუნველყოფა.

თავდაჯერებულობის ნაკლებობასთან გამკლავება – ლიდერები წარმატებით წყვეტენ თავდაჯერებულობის ნაკლებობის გამოწვევას, რაც ახალდანიშნული ხელმძღვანელებისთვის განსაკუთრებით პრობლემურია. უცხო, კომპლექსური თემები, უცნობი გუნდი, საქმის სირთულე და სხვა ფაქტორები, ხშირად ყველაზე გამოცდილ პროფესიონალებსაც უქმნით

დისკომფორტს. ამ დროს, ხშირია შეცდომები, როდესაც ხელმძღვანელი პირები დაუმსახურებელ ან არაარსებით შენიშვნებზე აკეთებენ აქცენტს, ერიდებიან კვალიფიციურ ადამიანებთან ურთიერთობას და უნებურად შემოიკრებენ ხოლმე შედარებით დაბალი კვალიფიკაციის თანამშრომლებს, რომლებთანაც თავს უფრო კომფორტულად გრძნობენ.

ლიდერები რთულ სიტუაციებშიც ახერხებენ თანამშრომლების ნდობისა და პატივისცემის მოპოვებას. მათ განსაკუთრებით გამოარჩევთ მხარდაჭერა იმ შუა რგოლის მენეჯერებისთვის, რომლებიც, შესაძლოა, მსგავსი გამოწვევების წინაშე არიან შესაბამის სტრუქტურულ ერთეულში. მართვასთან დაკავშირებული პრობლემების გადაწყვეტაში დახმარება ლიდერების ერთ-ერთი უმნიშვნელოვანესი ფუნქციაა.

ლიდერობის გავრცელებული თეორიები და მიდგომები

ჯონ მაქსველი – ლიდერობის ხუთი დონე

ლიდერობა არ არის ერთი კონკრეტული მოცემულობა, მას შეიძლება მრავალი ფორმა და განვითარების გზა ჰქონდეს. ჯონ მაქსველი გამოყოფს ლიდერობის ხუთ საფეხურს, ხუთ დონეს:

ლიდერობის პირველი დონე. მაქსველი ლიდერობის ყველაზე დაბალ საფეხურად პოზიციურ ლიდერობას ასახელებს – მდგომარეობა, როდესაც ხელმძღვანელს დანარჩენი თანამშრომლები მხოლოდ მისი მაღალი იერარქიული პოზიციის გამო ემორჩილებიან. მენეჯერებს ხშირად არასწორად ჰგონიათ, რომ რადგან მათ მინისტრის, მოადგილის, თავმჯდომარის და სხვა მაღალი თანამდებობები ერგოთ, „უსიტყვო მორჩილება“ გარანტირებული უნდა ჰქონდეთ და თუ ასე არ ხდება, ეს თანამშრომლის პრობლემაა. სინამდვილეში, რამდენად დამყოლნი და საქმის კარგად შემსრულებელნი იქნებიან თანამშრომლები, სხვა მნიშვნელოვან ფაქტორებთან ერთად, დამოკიდებულია მათივე მოტივაციაზე, რისთვისაც მხოლოდ ხელმძღვანელი პირის მითითება არ კმარა.

მაქსველის მიხედვით, ორგანიზაციებში, სადაც ძირითადად პოზიციური ლიდერობაა გავრცელებული, ადამიანები მუშაობენ ვალდებულების, ხელფასის ან სამსახურის დაკარგვის შიშის გამო, ისინი არ არიან იდეის, ორგანიზაციის ერთგულები. შესაბამისად, ადვილი შესამჩნევია როგორ ელოდებიან თანამშრომლები დღის ბოლოს, რომ დროულად წავიდნენ სამსახურიდან, ნაადრევად იწყებენ მაგიდის მოწესრიგებას, კოლეგებთან საუბარს, მაქსიმალურად ცდილობენ, ყველა პირადი საქმე შეძლებისდაგვარად სამსახურის დროის ხარჯზე მოაგვარონ. შესაბამისად, ორგანიზაციისთვის გაიღებენ იმ მინიმალურ დროსა და ენერგიას, რაც კუთვნილი ანაზღაურების სტაბილურად მისაღებად და სამსახურის შესანარჩუნებლად კმარა.

ორგანიზაციის ხელმძღვანელები ხშირად ვერ აცნობიერებენ, რომ ეს უმოტივაციობა, ზოგჯერ დაუმორჩილებლობაც მათი დამოკიდებულების ბრალია, უპირველეს ყოვლისა – მათ ვერ მოახერხეს ლიდერობის შემდეგ დონეზე გადასვლა.

ლიდერობის მეორე დონე. ლიდერობის მეორე დონეზე თანამშრომლები საკუთარი ნებით და არა ვალდებულებით მიჰყვებიან ხელმძღვანელს. თანამშრომლებს მოსწონთ ხელმძღვანელთან მუშაობა, ურთიერთობა და აღიარებენ ორგანიზაციის ლიდერად. ამისათვის აუცილებელია, რომ ხელმძღვანელმა კარგი ურთიერთობები დაამყაროს თანამშრომლებთან. საამისოდ რამდენიმე გზა არსებობს: დავინტერესდეთ, როგორ გრძნობენ თავს თანამშრომლები, მოვუსმინოთ, გამოვხატოთ ემპათია, დავანახვოთ, რომ ჩვენთვის ყოველი მათგანი მნიშვნელოვანია და ყურადღება გამოვიჩინოთ მათი როგორც პირადი, ასევე სამსახურში არსებული გამოწვევების მიმართ.

ლიდერობის მესამე დონე. მესამე საფეხურზე ლიდერები ახერხებენ, საკუთარი მაგალითით გახდნენ მოტივაციისა და ინსპირაციის წყარო დანარჩენი თანამშრომლებისთვის – საკუთარი მუშაობის სტილით, პროდუქტიულობით, ეფექტურობით, მაღალი ეთიკური სტანდარტით და ა.შ. ამ დონეზე, ორგანიზაცია აღწევს პროდუქტიულობის მაღალ ხარისხს, რადგან ყველას სურს, საკუთარი ძალისხმევა დაუკავშიროს ორგანიზაციის წარმატებას. ამ ეტაპზე კარგი ურთიერთობები ყალიბდება თანამშრომლებს შორისაც. როგორც ამბობენ, ამ ეტაპზე ორგანიზაციული პრობლემების 80% მაღალი სამუშაო ტემპის, კარგი ლიდერობისა და სწორი ორგანიზაციული კულტურის ხარჯზე გვარდება. ადამიანები ნაკლებად ინტერესდებიან შესაძლო უსამართლობებით, სამუშაო პირობებს შორის განსხვავებებით, ნაკლებად ეძებენ უკმაყოფილების მიზეზებს და მიმართულნი არიან ერთი მხრივ, საკუთარ დავალებებზე, ხოლო მეორე მხრივ, ორგანიზაციული დონის მიზნებზე.

აღსანიშნავია, რომ მესამე დონეზე ლიდერები ახერხებენ ორგანიზაციული კულტურის შეცვლას, დროთა განმავლობაში, იზიდავენ საკუთარი ღირებულებებისა და მიდგომების მქონე ადამიანებს ორგანიზაციაში, ხოლო ორგანიზაციას თანდათან ტოვებენ სხვა ფასეულობებისა და დამოკიდებულებების მატარებელი კოლეგები.

ლიდერობის მეოთხე დონე. ამ ეტაპს ჯონ მაქსველი თანამშრომელთა განვითარების დონეს არქმევს. ლიდერი ზრუნავს და ახერხებს თანამშრომელთა პროფესიონალიზმის ზრდის, განვითარების ხელშეწყობას. ასევე, არჩევს სწორი კვალიფიკაციისა და უნარების თანამშრომლებს, სწორად ანაწილებს დავალებებს კომპეტენციებისა და ინტერესების შესაბამისად, ასევე ანაწილებს პასუხისმგებლობებს და ქმნის პირობებს, რომელთა მეშვეობითაც თანამშრომლები საკუთარ შესაძლებლობებს საუკეთესოდ ავლენენ.

ლიდერობის აღნიშნულ საფეხურზე ადამიანებს მიაჩნიათ, რომ კონკრეტულ ხელმძღვანელთან ერთად მუშაობა მათთვის კარგია, ხელს უწყობს მათ განვითარებას და დადებითად აისახება მათ მომავალზე. ამ ეტაპზე, შესაძლებელია, შუა და შედარებით დაბალ იერარქიულ საფეხურზე მყოფი თანამშრომლები თავად იქცნენ ლიდერებად, მენტორებად სხვა თანამშრომლებისთვის და ხელი შეუწყონ, ასევე, კოლეგების მოტივაციას.

ლიდერობის მეხუთე დონე. მეხუთე საფეხური ლიდერობის უმაღლესი ეტაპია – ამ მოცემულობაში თანამშრომლები პატივს სცემენ ხელმძღვანელ პირს და თითქმის უსიტყვოდ მიჰყვებიან მას. ეს ნიშნავს, რომ ლიდერმა თანმიმდევრულად, დიდი ხნის განმავლობაში აჩვენა

სწორი გადაწყვეტილებები, კვალიფიკაცია, ემპათია, მაღალი ხარისხით განხორციელებული პროდუქტები და ამ საყოველთაო აღიარების ნაწილი სხვებიც არიან.

ცხადია, ხელმძღვანელი პირები სხვადასხვა თანამშრომელთან ლიდერობის განსხვავებულ დონეზე არიან. შესაბამისად, მნიშვნელოვანია, ლიდერი მუდმივად ცდილობდეს, რაც შეიძლება ბევრ თანამშრომელთან მიაღწიოს ლიდერობის მაღალ ხარისხს, რადგან დამკვიდრდეს შესაბამისი ორგანიზაციული კულტურა და ურთიერთობები, რაც უზრუნველყოფს წარმატების მომტანი, ეფექტური სამუშაო პროცესების მდგრად დამკვიდრებას.

ჯეიმს მაკგრეგორ ბიორნსი – ტრანზაქციული და ტრანსფორმაციული ლიდერობა

ჯეიმს მაკრეგორ ბიორნსმა ლიდერობის ორი განსხვავებული სტილი აღწერა:

ტრანზაქციული ლიდერობა – მეტწილად გულისხმობს არსებული პროცესების გამყარებას, მკაცრ კონტროლს და მართვის შედარებით ხისტ სტილს. ლიდერობის ამ სტილს ბიორნსი ტრანზაქციულს უწოდებს, რადგან ლიდერსა და მიმდევრებს შორის ხდება ერთგვარი ტრანზაქცია, გაცვლა: ლიდერის მხრიდან – გარკვეული წამახალისებელი მექანიზმები, მატერიალური ან არამატერიალური ჯილდო, მიმდევრების მხრიდან – დაკისრებული დავალებების ზედმიწევნით კარგად შესრულების სანაცვლოდ;

ტრანსფორმაციული ლიდერობა – აღწერს ლიდერობის ისეთ სტილს, როდესაც ხელმძღვანელები ორიენტირებულნი არიან მუდმივ ცვლილებებზე, განვითარებაზე, ორგანიზაციის მიზნების, პროდუქტების, მომსახურების გაუმჯობესებაზე. შესაბამისად, ტრანსფორმაციული ლიდერები მუდმივად ახალ, ამბიციურ ამოცანებს უსახავენ თანამშრომლებს. ტრანზაქციული ლიდერობისგან განსხვავებით, ამ შემთხვევაში, თანამშრომლები ჯილდოს იღებენ ახალი ინიციატივების, მეტი პასუხისმგებლობის, ახალი იდეების, ახალი მიზნების წარმატებით თავის გართმევის შემთხვევაში.

თუ აღნიშნულ თეორიას მაქსველის ლიდერობის ხუთ დონეს დავუკავშირებთ, ტრანზაქციული ტიპი მეტწილად ემყარება პოზიციურ ლიდერობას და მიმდევრების მორჩილებას არსებული პროცესების, დავალებების განსახორციელებლად, ტრანსფორმაციული ლიდერობა კი მეტად საჭიროებს მიმდევრებსა და ლიდერს შორის საერთო ფასეულობების, ღირებულებებისა და მიზნების გარშემო გაერთიანებას და ცვლილებებისკენ ერთად სვლას.

ცხადია, ლიდერობის აღნიშნული ორი ტიპი ერთმანეთს არ გამორიცხავს და შესაძლოა ხელმძღვანელებში სხვადასხვა ხარისხით, სიმკვეთრით იყოს გამოხატული.

ჰერსი და ბლანშარი – სიტუაციური ლიდერობა

სიტუაციური ლიდერობის თეორიის ფუძემდებლები, ჰენსი და ბლანშარი, აღნიშნავენ, რომ არ არსებობს ლიდერობის ერთი საუკეთესო, უნივერსალური გზა და ლიდერობა კონკრეტული გარემოს, მოცემულობის მიხედვით და თავისებურებების გათვალისწინებით უნდა განხორციელდეს. გარკვეულწილად ამითვე აიხსნება, რომ ერთი და იგივე ადამიანები სხვადასხვა ტიპის ორგანიზაციაში ან თუნდაც განსხვავებულ პოზიციებზე ერთნაირი წარმატებით მუშაობას ვერ ახერხებენ. ავტორები[9] ლიდერობის ოთხ შესაძლო ტიპზე ამახვილებენ ყურადღებას, რომელიც ძირითადად გადაწყვეტილების მიღების ალტერნატიულ მიდგომებს ეფუძნება:

დემოკრატიული ლიდერები გადაწყვეტილებას თანამშრომელთა უკუკავშირის მიღებით, მათი მონაწილეობით იღებენ და საკუთარ როლს მენეჯერების მხარდაჭერაში ხედავენ;

ავტოკრატიული ლიდერები ერთპიროვნულ გადაწყვეტილებებს ანიჭებენ უპირატესობას და, ძირითადად, ინსტრუქციების, დირექტივების გაცემაზე არიან ორიენტირებულნი;

დელეგირებაზე ფოკუსირებული, თავისუფალი მართვის სტილის (laissez-fair) ლიდერები მათზე დაბალ იერარქიულ საფეხურზე მყოფ თანამშრომლებს ანდობენ მსხვილ, მნიშვნელოვან გადაწყვეტილებებს.

თანამონაწილეობითი მართვის სტილისთვის გადაწყვეტილების მიღებისას ძირითადი ინსტრუმენტი თანამშრომელთა დარწმუნებაა.

ავტოკრატიული ლიდერობა ალბათ ნაკლებად შეიძლება ჭეშმარიტ ლიდერობად ჩაითვალოს, რადგან იგი მეტწილად მხოლოდ პოზიციურ ძალაუფლებას ეფუძნება და ხშირად ნაკლებეფექტიანია. დემოკრატიული ლიდერობა უმეტესად გადაწყვეტილებების მიღების ყველაზე წარმატებულ მოდელად განიხილება. რაც შეეხება დელეგირებაზე ორიენტირებულ ხელმძღვანელებს, ამგვარი მიდგომა მეტად პატარა გუნდებში ან ე.წ. „სტარტ-აპ“ გარემოშია მიზანშეწონილი, როდესაც მცირე მასშტაბების გამო კარგი კოორდინაცია, ინფორმაციის ეფექტიანი გაცვლა, ქვედა დონეზე სწრაფი გადაწყვეტილებები, კუთვნილება და მხარდაჭერა გადამწყვეტ მნიშვნელობას იძენს წარმატებისთვის. თუმცა, ორგანიზაციის ზომის ზრდასთან ერთად, ხშირად ორგანიზაცია მეტად იერარქიულ სტრუქტურას იღებს, სტაბილური ხარისხისა და თანმიმდევრულობის უზრუნველსაყოფად სტანდარტული პროცესებისა და პროცედურების მნიშვნელობა იზრდება.

ფრედერიკ ფიდლერი – დამოკიდებულების თეორია

დამოკიდებულების თეორიის მიხედვით, წარმატება მნიშვნელოვნადაა დამოკიდებული იმაზე, თუ რამდენად აუღებს ალღოს ლიდერი არსებულ გამოწვევებს, გარემოს და შესაბამისად იმოქმედებს. ფიდლერი განასხვავებს მეტწილად ურთიერთობებით (relationship orientation)

[9] ჰერსი და ბლანშარდი მცირედ განსხვავებულ მიდგომებს გვთავაზობენ, თუმცა აქ შეჯამებულია მათი თეორიის ძირითადი მიდგომები.

ან საქმით (task orientation) მოტივირებულ ლიდერებს. პირველ შემთხვევაში ხელმძღვანელებისთვის პრიორიტეტულია ურთიერთობები თანამშრომლებთან და მხოლოდ ურთიერთობებში აღქმული წარმატების მიღწევის შემდეგ კონცენტრირდება დავალებებისა და ამოცანების შესრულებასა თუ კონტროლზე. მეორე მხრივ, არიან ლიდერები, რომლებიც მეტწილად დავალებების შესრულებაზე არიან ორიენტირებულნი და ურთიერთობები შედარებით მეორეხარისხოვნად მიაჩნიათ. ცხადია, არ არსებობენ სრულად ურთიერთობებზე ან საქმეზე ორიენტირებული ლიდერები, თუმცა მათ სწორედ ის განასხვავებთ, თუ რას ანიჭებენ უპირატესობას.

ზოგჯერ ცალკე გამოყოფენ ქარიზმატულ ლიდერობასაც, როდესაც ლიდერობის, გავლენის ძირითადი წყარო ადამიანის ქარიზმიდან მომდინარეობს. თავის მხრივ, ქარიზმა ყველა ტიპისა და მიდგომის ლიდერებს უწყობს ხელს, გავლენა მოახდინონ მიმდევრებზე.

ელექტრონული ლიდერობა: შესაძლებლობები და გამოწვევები

ტექნოლოგიების როლის სწრაფი ზრდისა და ციფრული რევოლუციის ფონზე, ორგანიზაციული წარმატების ასპექტში ელმმართველობის მნიშვნელობაზე არავინ დავობს. მრავალი შეფასება და კვლევა გვიჩვენებს, როგორ შეიძლება ელექტრონული გადაწყვეტილებების სწორად დანერგვით გავაუმჯობესოთ მართვის პრაქტიკა ადამიანური რესურსების, ფინანსური აღრიცხვისა და ანგარიშგების, კომუნიკაციისა და მარკეტინგის, მომხმარებლებთან უკუკავშირის, პროდუქტების წარმოებისა და მიწოდების, მონიტორინგისა და შეფასების და სხვა ორგანიზაციული საქმიანობის ჭრილში. ზოგადი ტენდენციის მიუხედავად, ტექნოლოგიების როლი ლიდერული ფუნქციების უკეთ განხორციელების, ლიდერისა და მიმდევრების ურთიერთობის კონტექსტში შედარებით ნაკლებ შესწავლილია და მხოლოდ მოგვიანებით დაიწყეს მისი კვლევა. თანამედროვე პერიოდში პანდემიისგან გამოწვეულმა დისტანციური მუშაობის პრაქტიკის დანერგვამ, კომუნიკაციის ელექტრონული საშუალებების კიდევ უფრო ფართოდ გამოყენებამ და ხშირად მისმა უალტერნატივობამ, ამ პროცესს განსაკუთრებით შეუწყო ხელი.

ელლიდერობის ერთი უნივერსალური განმარტება, გაგება არ არსებობს. თუმცა, ვთანხმდებით, რომ ელლიდერობა გულისხმობს ისეთი საკითხების კვლევას, როგორებიცაა:

- რა როლს ასრულებს ტექნოლოგიები ლიდერობის განხორციელებისას?
- რა ტიპის გამოწვევები ან შესაძლებლობები ჩნდება ლიდერებისთვის მიმდევრებთან ურთიერთობის კონტექსტში?
- რა კომპეტენციები და უნარები სჭირდებათ წარმატებულ ლიდერებს თანამედროვე სამყაროში, რომელშიც ტექნოლოგიებზე დამოკიდებულება მუდმივად იზრდება?

ელლიდერობასთან დაკავშირებული თანმდევი მნიშვნელოვანი საკითხია დისტანციურად მუშაობის პრაქტიკა, რაც დროთა განმავლობაში, ყველა სექტორში მზარდი ტენდენციით ხასიათდებოდა. კერძო სექტორში საინფორმაციო ტექნოლოგიები, მარკეტინგი და ა.შ. ის სფეროებია, რომლებშიც მრავალი წელია ხშირად ე.წ. ტელევორკინგს – დისტანციურ მუშაობას მიმართავდნენ. საჯარო სექტორს, ცხადია, მეტი დრო დასჭირდა მოქნილობის გამოსავლენად და მსგავსი პრაქტიკა მეტწილად სსიპ-ის ტიპის სააგენტოებში გვხვდებოდა. დისტანციური მუშაობის გავრცელება მნიშვნელოვნად დააჩქარა პანდემიამ და დღევანდელი გადმოსახედიდან ძნელი წარმოსადგენია, რომ ორგანიზაციები სრულად დაუბრუნდებიან პანდემიის წინა მდგომარეობას.

რატომ არის აუცილებელი ლიდერობის როლის გადააზრება ელმმართველობის კონტექსტში? მიუხედავად კონკრეტული ლიდერის გემოვნებისა, პრეფერენციებისა და უნარებისა, გვერდს ვერ ავუვლით შემდეგ ფაქტებს:

ელმმართველობა და ტექნოლოგიების გამოყენება მხოლოდ ვიწრო სპეციალობა აღარ არის. ტექნოლოგიების უკეთ ცოდნა და სწორად გამოყენების უნარი სულ უფრო აქტუალური ხდება ორგანიზაციის ნებისმიერ იერარქიულ საფეხურზე მყოფი თანამშრომლისთვის. ეს განსაკუთრებით მნიშვნელოვანია ხელმძღვანელი პირებისთვის, რომელთა პასუხისმგებლობა არა მხოლოდ ტექნოლოგიების წარმატებით გამოყენება, არამედ სტრატეგიული გადაწყვეტილებების მიღებაცაა იმაზე, თუ რა ტიპის ტექნოლოგიები უნდა დაინერგოს, როგორ უნდა მოხდეს ეს, შესაბამისი უნარების განვითარება, თანამშრომელთა კვალიფიკაციის ზრდა, საჭიროებების გამოვლენა და ა.შ. ხშირად, ლიდერებს არასწორად წარმოუდგენიათ, რომ ამ საკითხების სრულად დელეგირება რომელიმე მოადგილეზე ან IT დეპარტამენტზე შეიძლება, რაც არასწორია. მხოლოდ ელფოსტა, ცნობილი საოფისე პროგრამები და ინტერნეტში მუშაობის უნარი ორგანიზაციული განვითარებისთვის აღარ კმარა.

ეფექტიანი კომუნიკაციის მნიშვნელობას ლიდერობის კონტექსტში შესაბამის ლიტერატურაში ყოველთვის განსაკუთრებული მნიშვნელობა ენიჭებოდა. დისტანციური მუშაობის პოპულარიზაციამ, რაც პანდემიამდე დაიწყო, მაგრამ პანდემიის შედეგად განსაკუთრებით მასშტაბური და პოპულარული გახდა, შეუდარებლად გაზარდა და უალტერნატივოდ აქცია ტექნოლოგიების როლი კომუნიკაციაში. ბოლო წლების განმავლობაში მრავალი ტიპის საკომუნიკაციო საშუალება განვითარდა. შესაბამისად, ლიდერებმა სწორი არჩევანი უნდა გააკეთონ და მიხვდნენ, რა ტიპის საკომუნიკაციო არხები იქნება ყველაზე ეფექტიანი და წარმატების მომტანი.

გარდა ლიდერისა და მიმდევრების კომუნიკაციისა, ცხადია, დისტანციური მუშაობის თანმდევად განვითარდა გუნდების, ჯგუფების ელკოლაბორაციის მექანიზმები, როგორებიცაა დოკუმენტების ელექტრონული სანახები, უფრო ფართო გამოყენება, ონლაინ კოლაბორაციის ინსტრუმენტები, ელკოორდინაციის, მონიტორინგის, დაგეგმვისა და სხვა საშუალებე-

ბი. დისტანციური მუშაობის პოპულარიზაციის შედეგად, აღნიშნული გადაწყვეტები კიდევ უფრო მნიშვნელოვანი და უალტერნატივო გახდა ორგანიზაციული საქმიანობისთვის.

ელექტრონული გადაწყვეტილებები ლიდერებისთვის მრავალ ახალ შესაძლებლობას აჩენს:

პირადი კომუნიკაცია ერთდროულად ბევრ თანამშრომელთან. ტრადიციულად, ისეთი მნიშვნელოვანი საკითხები, როგორებიცაა ორგანიზაციის მისია, ხედვა, არსებითი სტრატეგიული გადაწყვეტილებები, თანამშრომლებს წერილობითი ფორმით, ან შესაბამისი მენეჯერების გავლით გადაეცემათ. ცხადია, ინფორმაციის გადაცემისას ხდება ინტერპრეტირება და ინფორმაციის ან აქცენტების გარკვეული ცვლილება. ამ მხრივ, კომუნიკაციის ელექტრონული საშუალებები განსაკუთრებით ეფექტიანია. ასე ლიდერებს შეუძლიათ, ათასობით თანამშრომელს პირადად გააცნონ სიახლეები, სტრატეგია და ხედვა, სამომავლო გეგმები და შესაბამისი პრიორიტეტით, ფოკუსით, ინსპირაციით გაუზიარონ ინფორმაცია. ამგვარი პრაქტიკის დანერგვას მნიშვნელობა აქვს თანამშრომელთა მოტივაციის მიზნითაც იქ, სადაც, განსაკუთრებით დიდ ორგანიზაციებში, შესაძლოა თანამშრომლები ორგანიზაციის ლიდერებს, პირველ პირებს ვერასდროს ხვდებოდნენ. ლიდერების მხრიდან თუნდაც მადლობის პირადად გადახდა შეიძლება მნიშვნელოვანი მოტივაცია აღმოჩნდეს თანამშრომლებისთვის და დადებითად აისახოს მათ მუშაობაზე.

კვალიფიციური კადრების მოზიდვა მიუხედავად გეოგრაფიული სიშორისა. ორგანიზაციებს შეუძლიათ, მათთვის სასურველი კვალიფიკაციისა და კომპეტენციის მქონე კადრები გეოგრაფიული შეზღუდვების გარეშე შეარჩიონ და დაასაქმონ. ეს ფაქტორი განსაკუთრებით გასათვალისწინებელია პატარა ქალაქებში, რომლებშიც დასაქმების ბაზარი ისედაც მცირეა და კომპეტენციები – შეზღუდული.

ხარჯების შემცირება. დისტანციური მუშაობის შედეგად ორგანიზაციები ამცირებენ ხარჯებს, რომლებიც უკავშირდება საოფისე ქირას (ბევრმა ორგანიზაციამ შეამცირა საოფისე სივრცე და თანამშრომლების ნაწილი მუდმივად დისტანციურ რეჟიმზე გადაიყვანა), ტრანსპორტირებას, ავტომანქანების სადგომს და ა.შ.

მწვანე ინიციატივები. სხვადასხვა ქვეყანაში დისტანციური მუშაობა ასევე დაკავშირებულია მწვანე ინიციატივებთან, რომ ტრანსპორტის ნაკლები გამოყენებით განიტვირთოს მოძრაობა და ნაკლები ზიანი მიადგეს გარემოს.

დისტანციური მუშაობის თანმდევ დადებით საკითხებად შეიძლება ჩაითვალოს სტრესის ნაკლები დონე – დასაქმებულების მნიშვნელოვანი ნაწილი აღნიშნავს, რომ მათთვის ნაკლებად სტრესულია არასაოფისე გარემოში, მოქნილი გრაფიკით მუშაობა. ასევე, არსებობს კვლევები, რომლებიც მოქნილ გრაფიკს კადრების მეტ სტაბილურობას და ნაკლებ გადინებას უკავშირებენ.

მიუხედავად ახალი შესაძლებლობებისა, არსებობს მნიშვნელოვანი გამოწვევებიც, რაც ვირტუალურ სამყაროში ლიდერობის განხორციელებას უკავშირდება:

კომუნიკაცია. ელექტრონული კომუნიკაციის დროს, ცხადია, შეზღუდულია არავერბალური კომუნიკაციის საშუალებები და, შესაბამისად, გაცილებით ძნელია ენთუზიაზმის, ინსპირაციის, ქარიზმის გადაცემა. აღსანიშნავია ისიც, რომ თანამშრომელთა უმეტესობას უჭირს ყურადღების

მობილიზება დიდი ხნის განმავლობაში, განსაკუთრებით კომუნიკაციის ელექტრონული საშუალებების გამოყენებისას, რასაც „საკომუნიკაციო გადაღლას“ უწოდებენ (communication fatigue).

ლიდერებმა უნდა მოახერხონ კომუნიკაციის ელექტრონული და ტრადიციული ფორმების შერჩევა სიტუაციისა და საჭიროების მიხედვით. არის შემთხვევები, როდესაც ტექნოლოგიების შესაძლებლობებით აღტაცებული ლიდერები ზედმეტად, ნებისმიერ სიტუაციაში ელექტრონული საშუალებების გამოყენებას ამჯობინებენ. სინამდვილეში, ყველა საკომუნიკაციო საშუალებას თავისი უპირატესობა და ნაკლი აქვს. შესაბამისად, სწორი კომუნიკაცია გულისხმობს მათ შორის სწორი, ყველაზე ეფექტიანი ფორმის შერჩევას. მაგალითად, სასურველი ტრენინგის ელექტრონულად თუ ფიზიკურ სივრცეში ჩატარება აჯობებს? ან იქნებ შერეული ფორმა იყოს მიზანშეწონილი ცოდნის საუკეთესოდ გადასაცემად და შემდეგ ცოდნის შესაფასებლად? ერთი მხრივ, უნდა ვიფიქროთ საუკეთესო ფორმის შერჩევაზე, ხოლო მეორე მხრივ, შერჩეული ფორმიდან გამომდინარე, ინფორმაციის მიწოდების ფორმატზე, ვიზუალური მასალის გამოყენებაზე, დროისა და ყურადღების ფოკუსირების თავისებურებებზე და სხვა.

ტექნიკური გაუმართაობა. ხშირია ტექნიკური პრობლემები, რომლებიც არასტაბილურ ინტერნეტს, გაუმართავ მოწყობილობებს ან მათ არასწორ გამოყენებას უკავშირდება. ეს ფრუსტრაციას, ყურადღების მოდუნებას და პროდუქტიულობის შემცირებას იწვევს. მსგავსი პრობლემები შესამჩნევი იყო პანდემიით გამოწვეულ დისტანციურ მუშაობაზე გადასვლისას, რაც ფორსმაჟორულ პირობებში, დაუგეგმავად და მოუმზადებლად მოხდა.

ტექნიკური კომპეტენციების ნაკლებობა. როგორც ხელმძღვანელ, ასევე სხვადასხვა იერარქიულ საფეხურზე მყოფ თანამშრომლებს შესაძლოა არ ჰქონდეთ შესაბამისი კომპეტენცია და ცოდნა, რათა ელექტრონული საშუალებების სწორად და ეფექტურად გამოყენებას გაართვან თავი, რაც, თავის მხრივ, იმედგაცრუებას და გადაღლას განაპირობებს.

არასათანადო სამუშაო გარემო. თანამშრომლებს, რომელთაც პანდემიასთან დაკავშირებით იძულებით მოუწიათ დისტანციურ რეჟიმზე გადასვლა, შესაძლოა არ ჰქონდეთ სახლიდან სამუშაოდ შესაფერისი პირობები. აღნიშნულის შესაფასებლად არაერთი ორგანიზაცია იყენებს სტანდარტულ კითხვარებს, რომ მოგვიანებით პრობლემები არ წარმოიშვას.

კოლაბორაციისა და კოორდინაციის სირთულე. გუნდებს შორის ეფექტური კოლაბორაცია და კოორდინაცია ერთ-ერთი მნიშვნელოვანი გამოწვევაა ყველა ორგანიზაციისთვის. ვირტუალურ სამყაროში აღნიშნული საკითხი კიდევ უფრო გაძნელებულია.

იმისათვის, რომ გამოწვევებს ეფექტურად გაუმკლავდნენ, ელლიდერებს შემდეგი ტიპის უნარების, კომპეტენციებისა და მიდგომების გამოყენება ესაჭიროებათ:

ეფექტური კომუნიკაციის უნარი. ენთუზიაზმისა და ინსპირაციის გადაცემა, სწორი კომუნიკაცია ერთ-ერთი უმნიშვნელოვანესი, კრიტიკული უნარია ლიდერებისთვის. ელექტრონული კომუნიკაციის დაგეგმვისას აუცილებელია, ლიდერებმა უფრო მეტად კონკრეტული, ლაკონიური, მკვეთრი, ნათელ გზავნილებზე დაფუძნებული კომუნიკაცია აწარმოონ. ლიდერებს გაცილებით მეტი ცოდნა და ძალისხმევა სჭირდებათ, რომ სათანადოდ ჩაანაცვლონ კომუნიკაციისა და ინფორმაციის

გაცვლის ყველა ის ნიუანსი, რომლებსაც შეხვედრებზე, სამუშაო მაგიდებთან, დერეფნებში და სხვა საოფისე სივრცეებში იყენებდნენ.

სოციალური უნარები. ელლიდერებს განსაკუთრებული ძალისხმევა სჭირდებათ, რომ მიმდევრებისადმი თანაგრძნობა, მხარდაჭერა, თანადგომა გამოხატონ, მოიპოვონ ნდობა და გახდნენ მათი შთაგონებისა თუ მოტივაციის წყარო. ნდობის მოპოვება მნიშვნელოვანი გამოწვევაა დისტანციური მუშაობის დროს, რაც ლიდერებისთვის გადამწყვეტია. თანამშრომლებზე ზრუნვის, უშუალობის განცდა გაცილებით ნაკლებია ელსაშუალებებით კომუნიკაციის დროს, რადგან ის მეტად ფორმალური ხასიათისაა.

ტექნიკური კომპეტენციები. აუცილებელია, ლიდერებმა უზრუნველყონ როგორც საკუთარი, ისე ორგანიზაციაში, იერარქიის ნებისმიერ საფეხურზე მყოფი თანამშრომლის სათანადო ტექნიკური კომპეტენციის საკითხები. ამ მხრივ, საჭიროებების გამოვლენა და მუდმივი განვითარება, ტრენინგები, განსაკუთრებულ მნიშვნელობას იძენს ელექტრონული შესაძლებლობების ეფექტურად გამოყენების ჭრილში. პანდემიამ კიდევ ერთხელ დაადასტურა, რომ ხშირ შემთხვევაში ორგანიზაციის არც ლიდერები, და არც მიმდევრები სათანადო ცოდნას არ ფლობდნენ.

გუნდების განვითარების უნარი. ტრადიციული სამუშაო გარემოსგან მოწყვეტა ბევრისთვის მნიშვნელოვანი სირთულეა, რაც ფორმიდან ამოვარდნას და ეფექტურობის შემცირებას იწვევს. დისტანციური მუშაობა და მოქნილი გრაფიკი განსაკუთრებით პრობლემურია სუსტი თვითდისციპლინის მქონე თანამშრომლებისთვის. ლიდერებმა უნდა გაიაზრონ ის სიძნელეები, რომლებსაც არსებული და ახალი თანამშრომლები აწყდებიან და დაგეგმონ გუნდების მაინტეგრირებელი, შემაკავშირებელი ღონისძიებები.

ასევე გასათვალისწინებელია სამუშაო ბალანსის დარღვევით გამოწვეული, თანამშრომელთა ექსპლუატაციასთან დაკავშირებული რისკები. დისტანციურად მუშაობის პოპულარიზაციამ ბევრად უფრო ბუნდოვანი გახადა ზღვარი სამსახურსა და პირად ცხოვრებას შორის. თანამშრომლები და მენეჯერები აღნიშნავენ, რომ მათ გაცილებით მეტხანს და არანორმირებულად უწევთ მუშაობა. მსგავსი პროცესების ჩვეულ პრაქტიკად ქცევა გრძელვადიან პერსპექტივაში აუცილებლად გამოიწვევს თანამშრომელთა გადაღლას, დემოტივაციას და პროდუქტიულობის შემცირებას.

როგორ აისახება აღწერილი გარემოებები ლიდერობის სხვადასხვა სტილზე და მის პრაქტიკულ განხორციელებაზე?

ახალი გამოწვევების ფონზე ტრანსფორმაციული ლიდერობა განსაკუთრებით გართულებულია და მნიშვნელოვან დამატებით ძალისხმევას მოითხოვს. როგორც აღინიშნა, ტრანსფორმაციულ ლიდერობას სჭირდება ქარიზმა, თანამშრომელთა ინსპირაცია, მათზე ზრუნვისა და უშუალობით, მხარდაჭერითა და გვერდში დგომით ნდობის მოპოვება, რაც ვირტუალურ გარემოში შეზღუდული ან არსებითად სახეცვლილია. შესაბამისად, არის ტენდენცია, რომ ლიდერები უფრო მეტად ტრანზაქციული მოდელისკენ იხრებიან. ისინი მეტ

ყურადღებას აქცევენ მიმდინარე პროცესების, დავალებების კონტროლს, სტანდარტებისა და ხარისხის შენარჩუნებას და ამის სანაცვლოდ გასცემენ წამახალისებელ მატერიალურ თუ არამატერიალურ ჯილდოებს.

აღნიშნულის გააზრება მნიშვნელოვანია, რომ ორგანიზაციები დიდი ხნით არ ჩაიკეტონ მხოლოდ მიმდინარე პროცესების მართვაში და შეძლონ განვითარებაზე, სიახლეების დანერგვაზე, თამამ ინიციატივებზე ფიქრი, რასაც ტრანსფორმაციული ლიდერობა უწყობს ხელს.

სიტუაციური ლიდერობის მიდგომა ხაზს უსვამს, რომ ლიდერობის ერთი საუკეთესო გზა არ არსებობს. მას შემდეგ, რაც ხელმძღვანელები ლიდერობის შესაბამის მიდგომას შეარჩევენ, მათ უნდა გაითვალისწინონ, რა ელსაშუალებები ექნებათ ხელთ, რომ უზრუნველყონ მონაწილეობითობა, გუნდებს შიგნით და გუნდებს შორის კოლაბორაცია, დაგეგმონ შიდა კომუნიკაცია და გუნდების განვითარება, მათი უკეთესი ინტეგრაცია. დელეგირების, მონაწილეობითობისა თუ დემოკრატიული სტილის ლიდერებმა უნდა დაგეგმონ მათ მიერ შერჩეული მიდგომების შესაბამისი ღონისძიებები, პროცესები, განავითაროონ უკუკავშირისა და კოლაბორაციის არხები. აღნიშნული ძალისხმევა მნიშვნელოვანია, რომ თანდათანობით, გაძნელებული კომუნიკაციისა და კოორდინაციის ფონზე, ბუნებრივად არ განვითარდეს ავტოკრატიული მიდგომები და მასთან დაკავშირებული პროცესები.

აღნიშნული იმასაც გვაფიქრებინებს, რომ ვირტუალურ სივრცეში ლიდერობისას ხელმძღვანელებისთვის საკმაო გამოწვევაა ლიდერობის მაღალი ხარისხის მიღწევა. ამ დროს ყველაზე მკვეთრად პოზიციური ლიდერობაა გამოკვეთილი. შესაბამისად, უნდა დაიგეგმოს ისეთი კომუნიკაცია, რაც უზრუნველყოფს ნდობის, თანადგომის, მხარდაჭერის, ზრუნვისა და ემოციის განვითარებას მიმდევრების მხრიდან.

რაც შეეხება ფიდლერის დამოკიდებულების თეორიას, აღნიშნული მიდგომის მიხედვით, ლიდერების წარმატება და წარუმატებლობა სწორედ იმაზე იქნება დამოკიდებული, რამდენად კარგად მოერგებიან, ადაპტირდებიან ახალ გამოწვევებთან და რეალობასთან. თეორიის მიხედვით, ლიდერები მეტწილად საქმით (task orientation) ან ურთიერთობებით (relations orientation) არიან მოტივირებულნი. იქიდან გამომდინარე, რომ ურთიერთობებზე უარყოფითად აისახება ელსაშუალებების ფართო გამოყენება, ურთიერთობებით მოტივირებული ლიდერები შესაძლო გამოწვევის წინაშე დგებიან. მათ უნდა უზრუნველყონ ისეთი ალტერნატიული პროცესების განვითარება, რომლებიც ვირტუალური ურთიერთობებით გამოწვეულ სიცარიელეს შეავსებს.

შეჯამების სახით, შეიძლება ითქვას, რომ მიმდინარე გამოწვევების ფონზე, ლიდერებმა სწორად უნდა გააანალიზონ და შეაფასონ, რა შეიცვალა ფართო სურათში, როგორია ახალი ტენდენციები, რამდენად ეფექტურია თანამშრომელთა კომუნიკაცია, როგორია მათი კმაყოფილება და განწყობები, დამოკიდებულებები მიმდევრებსა და ლიდერებს შორის. დასკვნების საფუძველზე კი უნდა დაიგეგმოს კომპლექსური ღონისძიებები, ფართო ორ-

განიზაციული მიზნებიდან და ამოცანებიდან გამომდინარე, არსებული შესაძლებლობებისა და გამოწვევების გათვალისწინებით.

ელექტრონული მმართველობის დანერგვის წინაპირობები და ხელშემწყობი ფაქტორები

ელმმართველობის დანერგვის პროცესი ყველა ქვეყანაში სხვადასხვაგვარად მიმდინარეობს, რაზეც გადამწყვეტ გავლენას ახდენს ადგილობრივი გარემო და პრიორიტეტები. გამოყოფენ ციფრულ და ანალოგურ ხელშემწყობ ფაქტორებს.

ციფრული ხელშემწყობი ფაქტორებია:

წვდომა – თუკი მომხმარებლებს არ გააჩნიათ წვდომა ელექტროენერგიასა და ინტერნეტზე, შეუძლებელია ვისაუბროთ ელმმართველობის განვითარებაზე. ზოგიერთ ქვეყანაში ინტერნეტზე წვდომა ადამიანის უფლებად არის აღიარებული, მათ შორის, საქართველოშიც. საქართველოს კონსტიტუციით გარანტირებულია აზრის, ინფორმაციის, მასობრივი ინფორმაციის საშუალებათა და ინტერნეტის თავისუფლების უფლებები და მე-17 მუხლის მე-4 პუნქტის მიხედვით, ყველას აქვს ინტერნეტზე წვდომისა და ინტერნეტით თავისუფლად სარგებლობის უფლება.

ციფრული მონაცემთა ბაზები – მონაცემთა ბაზები გაციფრულებული და ხელმისაწვდომი უნდა იყოს ფიზიკური და იურიდიული პირებისთვის. მონაცემთა ბაზებში უნდა შედიოდეს სრული, სწორი და განახლებული ინფორმაცია/მონაცემები. მონაცემთა ბაზებში მონაცემთა დუბლირება უნდა გამოირიცხოს, რადგან დუბლირებული ბაზების არსებობა ადმინისტრაციულ ბარიერებს ზრდის. მონაცემთა ბაზებში არსებული მონაცემები ფიზიკური და იურიდიული პირების საკუთრებაა. ისინი აკონტროლებენ, როგორ მართავს მათ მონაცემებს სახელმწიფო. მონაცემთა ბაზებში არსებული მონაცემების ხარისხსა და უსაფრთხოებაზე პასუხისმგებლობა თითოეული უფლებამოსილ ორგანოს ეკუთვნის; სწორედ ამ მიზნით იქმნება ინფორმაციის ერთიანი სახელმწიფო რეესტრები, სადაც თავს იყრის ინფორმაცია საჯარო სექტორში არსებული რეესტრების, მონაცემთა ბაზების, მომსახურებისა და ინფორმაციული სისტემების შესახებ.

ურთიერთთავსებადი ინფრასტრუქტურა – მონაცემთა გაცვლის უსაფრთხო, ურთიერთთავსებადი ინფრასტრუქტურის მთავარი უპირატესობებია დუბლირებული მონაცემთა ბაზების თავიდან აცილებით უფლებამოსილ ორგანოთა მონაცემებზე დისტანციური წვდომა საჭიროებისამებრ: მონაცემთა ბაზების მხოლოდ ერთი, სანდო და ავთენტური პირველწყაროს არსებობა; ახალი სერვისების მარტივად შექმნა; ყველა ტრანზაქციის აღრიცხვა (ლოგირება) და დროის ბეჭდით (time stamp) აღნიშვნა;

ციფრული იდენტიფიკაციის საშუალებები – უზრუნველყოფს ონლაინსამყაროში პირთა იდენტიფიკაციას, მათ მიერ ტრანზაქციების განხორციელების შესაძლებლობას და სამოქალაქო ბრუნვის მდგრადობას ელექტრონულ სივრცეში. ძლიერი ციფრული იდენტიფიცირება აუცილებელია ციფრულ სამყაროში ფიზიკური და იურიდიული პირების ავთენტიფიკაციისთვის. ციფრული იდენტიფიცირება აუცილებელია როგორც სახელმწიფო, ასევე კერძო სექტორის ტრანზაქციებისთვის.

ის უნდა დაეყრდნოს მოქალაქეთა მონაცემების მართვის უტყუარ სისტემას და არ იყოს მისგან განცალკევებული;

მომსახურების პორტალები – პორტალი ტექნიკურად თავს უყრის მასზე ინტეგრირებულ ელექტრონულ სერვისებს. ვებრესურსები და მობილური აპლიკაციები ე.წ. „front-end“ სერვისებია, რომლებიც ვერ იფუნქციონირებენ „back-end“ გადაწყვეტების გარეშე. პორტალები ტრანზაქციებისთვის ერთიანი ანგარიშსწორების შესაძლებლობას უნდა იძლეოდეს;

კიბერუსაფრთხოება – უზრუნველყოფს კიბერინციდენტებისა და საფრთხეებისაგან ელექტრონული პროდუქტებისა თუ სერვისების დაცულობასა და უსაფრთხოებას, რაც ზრდის ამ უკანასკნელთა მიმართ მომხმარებელთა ნდობას და ელმმართველობის რეპუტაციას.

ანალოგურ ხელშემწყობ ფაქტორებს შორის მნიშვნელოვანია გამოვყოთ:

პოლიტიკური ნება – ელმმართველობა ერთიან სამთავრობო ხედვასა და ქვეყნის პოლიტიკურ პრიორიტეტებს უნდა ერგებოდეს;

სტრატეგიული ჩარჩო – ელმმართველობის სტრატეგია უნდა ასახავდეს პოლიტიკურ კურსს, ელმმართველობის სტრატეგია და ქვეყნის ICT – ინოვაციების, ეკონომიკური განვითარებისა და საჯარო მმართველობის სტრატეგიები – ერთმანეთს უნდა თანხვდებოდეს და ეთავსებოდეს. სტრატეგია ეროვნულ დონეზე შეთანხმებული გრძელვადიანი მიზნების, პრიორიტეტების, ჩარჩოებისა და ინფრასტრუქტურული პროექტების ერთობლიობაა, რომელიც შეესაბამება ზოგადად ქვეყნის საჯარო პოლიტიკას. სტრატეგია, როგორც ეროვნული დონის გზამკვლევი ელმმართველობის სფეროში, აღსრულებადი უნდა იყოს და ამ პროცესში ყველა დაინტერესებული მხარე უნდა იყოს ჩართული;

კანონმდებლობა და რეგულაციები – ელექტრონული მმართველობის უზრუნველმყოფი სამართლებრივი ბაზა. ტრადიციული სამართლებრივი პრინციპები და მოწყობა, როგორც წესი, არ ითვალისწინებს თანამედროვე უქაღალდო ოპერაციებისა და ვირტუალური პროცესების რეგულირებას, მოძველებული კანონები ხელს უშლის ელმმართველობის პროექტების განხორციელებას. საკანონმდებლო და მარეგულირებელი ბარიერების მოხსნა და საჯარო მომსახურების ტრანსფორმაცია ელმმართველობის განსავითარებლად პრიორიტეტად უნდა იქცეს. ელმმართველობის ხელშემწყობი სამართლებრივი ჩარჩოს შექმნა ელექტრონული სერვისების მისაწოდებლად და ონლაინ ტრანზაქციების განსახორციელებლად პრიორიტეტული მიმართულება უნდა გახდეს;

ფისკალური ჩარჩოები – ელმმართველობის პროექტები დაფინანსების გარეშე წარუმატებლობის წინაპირობაა;

მდგრადი ინსტიტუციურ-ორგანიზაციული სტრუქტურები – უფლებამოსილებების გამიჯვნა, კომუნიკაცია, კოორდინაცია და პარტნიორობა მკაცრად იდენტიფიცირებულ ორგანიზაციულ-სტრუქტურულ ერთეულებს შორის ელმმართველობის აუცილებელი წინაპირობაა. მკაფიო და ორგანიზებულად სტრუქტურირებული მმართველობითი მოდელი ელმმართველობის წარმატებით დანერგვის ერთ-ერთი მთავარი ხელშემწყობი გარემოა. ელმმართველობა საჭიროებს ქვეყანაში კოლაბორაციული მართვის სისტემის არსებობას და ადმინისტრაციული ორგანოების როლებისა და ფუნქციების ცალსახად განსაზღვრას სტრატეგიულ, ტაქტიკურ და ოპერაციულ დონეებზე.

ელექტრონული მმართველობა ორგანიზაციის მართვისა და განვითარებისთვის

ადამიანური რესურსების ელექტრონული მართვის სისტემები

რა არის ადამიანური რესურსების მართვა?

ადამიანური რესურსების მართვა გულისხმობს ციკლს, რომელიც მოიცავს შემდეგ ძირითადად პროცესებს: პერსონალის დაგეგმვა, შერჩევა, ადაპტაცია (ორიენტაცია), შესრულებული სამუშაოს მართვა და განვითარება. ადამიანური რესურსების მართვის როლი დღითიდღე იზრდება, პერსონალის შერჩევასა და ადმინისტრირებასთან ერთად იგი სტრატეგიული მნიშვნელობის ფუნქციებს იძენს. ორგანიზაციულ შედეგთან მიმართებით, სამუშაო ანალიზი ორ ძირითად მიმართულებას გვაჩვენებს: პერსონალის გარკვეული ნაწილი ჩართულია უშუალოდ შედეგების განსაზღვრასა და მიღწევაში, მეორე ნაწილს კი განხორციელების მხარდამჭერი ფუნქცია აკისრია. წარმატებულ ორგანიზაციებში გავრცელებული ტენდენციაა სტრატეგიული მიზნებისა და გეგმების შემუშავების პროცესში ადამიანური რესურსების მართვის ერთეულის ჩართულობის ზრდა.

აღნიშნულის მისაღწევად კონკრეტული გარემოებების შექმნაა საჭირო: 1. უმაღლესი მენეჯმენტის ინტერესი და ნდობა ადამიანური რესურსების მართვის მნიშვნელობის მიმართ. 2. ადამიანური რესურსების მართვაზე პასუხისმგებელი პირების მხრიდან მათი ფუნქციებისა და როლის გლობალური ხედვა ორგანიზაციული მიზნების განხორციელების ჭრილში. თუ ორივე ზემოხსენებული პირობა არსებობს, ადამიანური რესურსების მართვის ციკლის სრულყოფილად და წარმატებით განხორციელებისათვის დიდი ნაბიჯია გადადგმული.

ადამიანური რესურსების მართვის ელექტრონული სისტემები

ადამიანური რესურსების მართვა სათავეს XX საუკუნის ადრეული წლებიდან იღებს.[10] დღეს, როდესაც მთელმა მსოფლიომ არჩევანი დისტანციურად მუშაობის რეჟიმზე შეაჩერა, ბუნებრივია, ელექტრონული სისტემების გარეშე წარმოუდგენელია ადამიანური რესურსების შეუფერხებლად მართვა.

ადამიანური რესურსების მართვის ელექტრონული სისტემა (იგივე ადამიანური რესურსების ინფორმაციული სისტემა ან/და ადამიანური კაპიტალის მართვის ელექტრონული სისტემა) კომპიუტერული პროგრამებია, რომლებიც აერთიანებენ სხვადასხვა მიმართულებას და იმეორებენ ზემოხსენებულ სრულ ციკლს: დაგეგმვა, შერჩევა, ორიენტაცია, შესრულების მართვა და განვითარება. აღნიშნულ სფეროში ინფორმაციული ტექნოლოგიების გამოყენება 1970-იანი წლებიდან დაიწყო და თავდაპირველად, მიზნად ისახავდა ფეიროლის[11] ავტომატიზაციას და ადამიანური რესურსების მართვის პროცესის გამარტივებას. აღსანიშ-

[10] "Human resource management" – https://en.wikipedia.org/wiki/Human_resource_management#Antecedent_theoretical_developments.

[11] ფეიროლი – ხელფასების ადმინისტრირების სისტემა. პროცესი, რომლითაც დამსაქმებლები გასცემენ ხელფასსა და მასთან დაკავშირებულ განაცემებს დასაქმებულზე სამუშაოს შესრულებისათვის.

ნავია, რომ ელექტრონული სისტემების განვითარებას დასასრული არ აქვს და დღემდე განაგრძობს დახვეწა-გაუმჯობესებას.

ელექტრონული მართვის სისტემები საქართველოს საჯარო სამსახურში

ელექტრონული პლატფორმები საჯარო სამსახურში ადამიანური რესურსების მართვის ხელშეწყობის მიზნით გამოიყენება შერჩევის, პერსონალის ადმინისტრირების, შეფასებისა და პროფესიული განვითარების განსახორციელებლად, ასევე, სტაჟირების სახელმწიფო პროგრამის სამართავად.

კანონმდებლობა და პერსონალის შერჩევის ვებგვერდი (www.hr.gov.ge)

ვაკანტურ თანამდებობაზე კონკურსის ელექტრონულად გამოცხადების ვალდებულება „საჯარო სამსახურში კონკურსის ჩატარების წესის შესახებ“ საქართველოს მთავრობის 204-ე დადგენილებით არის დარეგულირებული. საჯარო დაწესებულება ღია, დახურულ და შიდა კონკურსს პროფესიული საჯარო მოხელის ვაკანტურ თანამდებობაზე აცხადებს ბიუროს მიერ ადმინისტრირებული ვებგვერდის (www.hr.gov.ge) მეშვეობით. ამასთანავე, საჯარო დაწესებულება უფლებამოსილია, ღია, დახურული ან შიდა კონკურსის გამოცხადების შესახებ ინფორმაცია დამატებით განათავსოს საჯარო დაწესებულების ვებგვერდზე, ხოლო ღია კონკურსის შემთხვევაში – ასევე შრომით ურთიერთობებთან დაკავშირებულ შესაბამის ვებგვერდებზე, სოციალურ ქსელებსა და ბეჭდვით ორგანოებში[12].

საჯარო სამსახურის კონკურსის ამოცანებია საჯარო სამსახურში არსებულ ვაკანტურ თანამდებობათა თანაბრად ხელმისაწვდომობის უზრუნველყოფა, ვაკანტური თანამდებობებისათვის კანდიდატების შერჩევისა და საჯარო სამსახურში განწესების პროცესის გამჭვირვალობის უზრუნველყოფა და საუკეთესო კანდიდატების შერჩევა ვაკანტური პოზიციებისათვის განსაზღვრულ ძირითად, სპეციალურ და ასევე, დამატებით საკვალიფიკაციო მოთხოვნებთან შესაბამისობის დადგენის გზით, კვალიფიკაციის, უნარ-ჩვევების, პროფესიული გამოცდილებისა და მოტივაციის შეფასების საფუძველზე. აღნიშნული ამოცანების განხორციელებას ხელს უწყობს ელექტრონული პლატფორმების გამოყენება.

პერსონალის შერჩევის ელექტრონული მართვა (www.hr.gov.ge)

ვებგვერდის (www.hr.gov.ge) მეშვეობით საქართველოს ნებისმიერ მოქალაქეს აქვს შესაძლებლობა, ონლაინ გააკეთოს განაცხადი საჯარო სამსახურში არსებულ ნებისმიერ ვაკანსიაზე და დასაქმდეს. ეს ერთადერთი გზაა კონკურსში მონაწილეობის მისაღებად და საჯარო სამსახურში კარიერის დასაწყებად. აღნიშნულ ვებგვერდზე დარეგისტრირებულია 297,808 სამსახურის მაძიებელი და 1150 საჯარო უწყება/დამსაქმებელი.[13]

---

[12] „საჯარო სამსახურში კონკურსის ჩატარების წესის შესახებ“ საქართველოს მთავრობის 204-ე დადგენილება, მუხლი 6.

[13] 2021 წლის 30 ივლისის მდგომარეობით.

Hr.gov.ge-ს რამდენიმე ტიპის სამომხმარებლო მხარე აქვს: 1. დამსაქმებელი ორგანიზაციის – საჯარო დაწესებულებებისათვის; 2. მოქალაქის – სამსახურის მაძიებლის; 3. ადმინისტრატორის – საჯარო სამსახურის ბიუროსათვის. ამასთანავე, ვებგვერდზე ფუნქციონირებს ონლაინდახმარება, რომლის მეშვეობითაც ნებისმიერ დაინტერესებულ პირს შეუძლია დააზუსტოს მისთვის სასურველი საკითხი ან/და მოკლე დროში გადაჭრას მის წინაშე არსებული ტექნიკური თუ სხვა სახის პრობლემა.

„საჯარო სამსახურის შესახებ“ საქართველოს კანონის შესაბამისად, ბიუროს ვალდებულება ამ ეტაპისთვის შემოიფარგლება ვებგვერდზე ვაკანსიების განთავსების ადმინისტრირებით. საკვალიფიკაციო მოთხოვნების დადგენა[14] და კონკურსის გამოცხადება[15] მხოლოდ დამსაქმებელი უწყების უფლებამოსილებაა.

სტაჟირების სახელმწიფო პროგრამა

სტაჟირების გავლის წესსა და პირობებს სახელმწიფო ხელისუფლების ორგანოებში, ადგილობრივი თვითმმართველობის ორგანოებსა და საჯარო სამართლის იურიდიულ პირებში განსაზღვრავს „საჯარო დაწესებულებაში სტაჟირების გავლის წესისა და პირობების შესახებ“ სახელმწიფო პროგრამის დამტკიცების თაობაზე“ საქართველოს მთავრობის 410-ე დადგენილება.

ამ პროგრამის ფარგლებში საჯარო დაწესებულებაში სტაჟირებას ფართო და მოცულობითი მიზანი აქვს: ა) საჯარო დაწესებულებაში დასაქმების მსურველ პირთათვის პროფესიული გამოცდილების შეძენის შესაძლებლობის შექმნა; ბ) შესაბამისი პროფილის სტუდენტებისა და კურსდამთავრებულებისათვის პრაქტიკული უნარ-ჩვევების გამომუშავების საშუალების მიცემა; გ) საჯარო დაწესებულებებისათვის კვალიფიციური კადრების მომზადება; დ) სტაჟირების ერთიანი სტანდარტის შემუშავება, რომელიც ხელს შეუწყობს სახელმწიფო სექტორში დასაქმების მსურველთათვის ჯანსაღი კონკურენციის შექმნასა და საჯარო სამსახურში დასაქმების ხელმისაწვდომობის უზრუნველყოფას; ე) სტუდენტებისა და კურსდამთავრებულებისათვის საჯარო მოსამსახურისათვის დამახასიათებელი ეთიკური ნორმებისა და სტანდარტების გაზიარება; ვ) სტუდენტებსა და კურსდამთავრებულებში დასაქმების შესაძლებლობების თაობაზე ცნობიერების ამაღლება; ზ) მაღალკვალიფიციური კადრების მოზიდვის გზით, საჯარო სამსახურის ერთიანი საკადრო პოლიტიკის გატარების ხელშეწყობა, საჯარო დაწესებულებების უზრუნველყოფა მოხალისე დამხმარე ძალით; თ) დასაქმების თანაბარი პირობების შექმნა როგორც რეგიონებში მცხოვრები პირებისათვის, ისე შეზღუდული შესაძლებლობის მქონე პირებისათვის.[16]

---

14 „საჯარო სამსახურის შესახებ“ საქართველოს კანონი, მუხლი 28.

15 „საჯარო სამსახურის შესახებ“ საქართველოს კანონი, მუხლი 35.

16 „საჯარო დაწესებულებაში სტაჟირების გავლის წესისა და პირობების შესახებ“ სახელმწიფო პროგრამის დამტკიცების თაობაზე“ საქართველოს მთავრობის 410-ე დადგენილება, მუხლი 2.

სტაჟირების სახელმწიფო პროგრამის მიზნების განსახორციელებლად შეიქმნა ვებგვერდი www.stajireba.gov.ge. ვებგვერდის მომხმარებლები არიან: 1. სტაჟირების მსურველები; 2. დამსაქმებელი ორგანიზაციები; 3. საჯარო სამსახურის ბიურო. მომხმარებელთა თითოეული ჯგუფისთვის ვებგვერდზე შექმნილია შესაბამისი განყოფილება.

პერსონალის ადმინისტრირების ელექტრონული სისტემა

რა არის პერსონალის ადმინისტრირება?

პერსონალის ადმინისტრირება ტრადიციული გაგებით, ძირითადად, გულისხმობს თანამშრომელთან შრომითი ურთიერთობის დაწყების, გათავისუფლების, წახალისების პროცესების მენეჯმენტს, დისციპლინური პასუხისმგებლობის დაკისრებისთვის საჭირო დოკუმენტაციის ორგანიზებას/მომზადებას, შვებულებებისა და მივლინებების მართვას, ფინანსური ანგარიშგებისთვის აუცილებელი ინფორმაციის გაერთიანებას, სამუშაო დროის აღრიცხვას, თანამშრომელთა დაზღვევისა და სხვა კორპორაციული მომსახურებების მართვას, ასევე, პირადი საქმეების წარმოებას.[17]

პერსონალის ელექტრონულად ადმინისტრირების საჭიროება

ჩამოთვლილთაგან თითოეული პროცესი განსაკუთრებულად მოითხოვს დეტალებზე ორიენტირებას, დიდ მატერიალურ რესურსს და დროს, რაც, თავის მხრივ, ორგანიზაციის ბიზნესპროცესების ეფექტიანობას რისკის ქვეშ აყენებს და ამასთანავე, ყოველდღიური, ერთგვაროვანი საქმიანობა ამცირებს ამ საკითხებზე დასაქმებული პირების შრომითი კმაყოფილებისა და მოტივაციის დონეს.

ხელით მართული რუტინის შესამცირებლად, უკვე დიდი ხანია მსოფლიო საზოგადოება და მათ შორის ქართული კერძო თუ საჯარო სექტორი აქტიურად ნერგავს სხვადასხვა ელექტრონულ პროგრამას, რათა პერსონალის ადმინისტრირების აუცილებელი პროცესების განსახორციელებლად რაც შეიძლება ნაკლები დრო და ადამიანური თუ მატერიალური კაპიტალი იყოს საჭირო.

კანონმდებლობა და პერსონალის ელექტრონულად ადმინისტრირება

პერსონალთან დაკავშირებული ინფორმაციის ელექტრონულად არსებობის ვალდებულება „საჯარო სამსახურის შესახებ“ საქართველოს კანონითაა განსაზღვრული. კერძოდ, საჯარო დაწესებულების ადამიანური რესურსების მართვის ერთეული პასუხისმგებელია ადამიანური რესურსების მართვის ერთიანი ელექტრონული სისტემის ფუნქციონირებისა

[17] თანამედროვე ინფორმაციული ტექნოლოგიები ეკონომიკური გლობალიზაციის პირობებში, თბილისი, 2015, გვ. 345

და მასში საქართველოს კანონმდებლობით განსაზღვრული ინფორმაციის ასახვაზე. მაგალითად, ელექტრონულად უნდა იყოს ასახული, მათ შორის, მოხელის კარიერულ განვითარებასთან დაკავშირებული მონაცემები, ასევე, ინფორმაცია მისთვის დისციპლინური პასუხისმგებლობის დაკისრებასთან დაკავშირებით.

აღნიშნული კანონის მიზანია ერთიანი საჯარო სამსახურის ჩამოყალიბებისა და ფუნქციონირების სამართლებრივი საფუძვლების შექმნა. ერთიანი საჯარო სამსახურის მიზნის მიღწევას მნიშვნელოვნად განაპირობებს ამ შემთხვევაში, პერსონალის ადმინისტრირების მიმართულებით არსებული ერთიანი მიდგომებისა და პრაქტიკის არსებობა, რაც, თავის მხრივ, გამოიხატება ერთიანი მონაცემთა ბაზის არსებობაში.

პერსონალის მართვის ელექტრონული პროგრამა

ამ გამოწვევის საპასუხოდ არის შექმნილი ადამიანური რესურსების მართვის ავტომატიზებული სისტემა (e-HRMS), რომელიც წარმოადგენს საჯარო დაწესებულებებში დასაქმებული პირების ერთიან მონაცემთა ბაზას და მიზნად ისახავს ადამიანური რესურსების ელექტრონული მართვის უზრუნველყოფას შესაბამის პოლიტიკასა და სტანდარტებზე დაყრდნობით.

ადამიანური რესურსების მართვის ავტომატიზებულ სისტემაში შესაძლებელია ორგანიზაციის სტრუქტურის აწყობა საშტატო ნუსხის საფუძველზე, შესაბამისი დაქვემდებარებებისა და პოზიციური კავშირების შექმნა. პროგრამის მეშვეობით შესაძლებელია თანამშრომელთა შესახებ მოცულობითი მატერიალური მასალის ელექტრონულად ასახვა და ელექტრონული პირადი საქმეების წარმოება, შესაბამისი დოკუმენტაციის მიბმა, სადაც პირის რეზიუმესთან ერთად, შესაძლებელია პოზიციის სამუშაოს აღწერილობით განსაზღვრული ფუნქციების, კომპეტენციებისა და საკვალიფიკაციო მოთხოვნების შესახებ ინფორმაციის მითითებაც.

ასევე აღსანიშნავია შვებულებებისა და მივლინებების შესახებ ინფორმაციის ელექტრონულ მონაცემთა ბაზაში ასახვის, შემდგომ დროულად დაჯამებებისა და შესაბამისი მიზნებისთვის გამოყენების შესაძლებლობაც.

მნიშვნელოვანია, რომ e-HRMS-ში არსებობს თანამშრომლის გარემო, ე.წ. „self-service“, რომელშიც სხვა ძირითად ინფორმაციასთან ერთად (ორგანიზაცია, პოზიცია, ტელეფონის ნომერი, ელფოსტა) წარმოდგენილია მონაცემები გამოყენებულ და დარჩენილ საშვებულებო დღეებთან დაკავშირებით, რაც ძალიან მოსახერხებელი და ადვილად ადმინისტრირებადია.

ამ ეტაპზე აღნიშნული პროგრამა პერსონალის ადმინისტრირების პროცესისთვის აუცილებელი საბაზისო მონაცემების დონეზე წარმატებით გამოიყენება საჯარო დაწესებულებების მიერ, თუმცა დახვეწას საჭიროებს სხვადასხვა მიმართულებით, რაზეც მუშაობა პერიოდულად გაგრძელდება.

საერთაშორისო და უკვე ქართული პრაქტიკის მიხედვით, მსგავსი ტიპის ელექტრონული პროგრამები აერთიანებენ თანამშრომელთა სამუშაო ადგილზე გამოცხადების, საერთოდ, ნამუშევარი საათების მონაცემებსაც; გარდა ამისა, ეს პროგრამები შესაძლებლობას იძლევა, თანამშრომლის გარემოდან თანამშრომელმა თავად მოითხოვოს შვებულება და სრული პროცესი ელექტრონულად იმართებოდეს.

ამგვარი ელექტრონული პროგრამების მთავარი წარმატება და გამოწვევა, ბიზნესპროცესების საგრძნობი გაუმჯობესებისა[18] და გამარტივების გარდა, არის ინფორმაციის სრულყოფილად ასახვა და დროული განახლება. სხვა შემთხვევაში პროგრამის სიკეთეებზე ვერ ვისაუბრებთ. ამ ნაწილში პასუხისმგებლობა თითოეულმა საჯარო დაწესებულებამ სათანადოდ უნდა გაიზიაროს.

პროფესიული განვითარება და პროფესიული განვითარების ელექტრონული სისტემა

ადამიანური რესურსების მართვის ციკლის ერთ-ერთი უმნიშვნელოვანესი კომპონენტი პერსონალის განვითარებაა. პერსონალის განვითარება შეიძლება აღვწეროთ, როგორც თანამშრომელთა სრულყოფის სისტემატური და უწყვეტი პროცესი, რომელიც ეხმარება მათ საკუთარი შესაძლებლობების მაქსიმალურად გამოყენებაში. აღნიშნული ერთი მხრივ, სასარგებლოა დასაქმებულისათვის, მეორე მხრივ კი ორგანიზაციისთვის.

მოხელის პროფესიული განვითარების წესს არეგულირებს „პროფესიული საჯარო მოხელის პროფესიული განვითარების საჭიროებების განსაზღვრის წესის, პროფესიული განვითარების სტანდარტისა და წესის დამტკიცების შესახებ“ საქართველოს მთავრობის N242 დადგენილება. მოხელის პროფესიული განვითარების საჭიროებებს საჯარო დაწესებულების უფლებამოსილი პირი განსაზღვრავს ყოველი წლის დასაწყისში, თითოეული მოხელის შეფასების შედეგებზე დაყრდნობით ან/და საჯარო დაწესებულების სტრატეგიული მიზნებისა და საჭიროებების გათვალისწინებით. საჯარო დაწესებულების ინტერესებიდან გამომდინარე, შესაძლებელია საჯარო დაწესებულების უფლებამოსილმა პირმა გადაწყვეტილება მიიღოს მოხელის პროფესიული განვითარების პროგრამაში მონაწილეობის თაობაზე, წლის ნებისმიერ დროს.

მოხელის პროფესიული განვითარების საჭიროება მოხელის მიერ უფლებამოსილებების განხორციელებისათვის აუცილებელი ცოდნისა და უნარების განვითარების საფუძველია საჯარო სამსახურში მაღალი პროფესიული სტანდარტის დამკვიდრებისა და საჯარო დაწესებულების გამართული ფუნქციონირების უზრუნველსაყოფად.

[18] თანამედროვე ინფორმაციული ტექნოლოგიები ეკონომიკური გლობალიზაციის პირობებში, თბილისი 2015, გვ. 261

პროფესიული განვითარების პროგრამების (საბაზისო და დამატებითი) გავლა შესაძლებელია სწავლების შემდეგი მეთოდებით/ფორმებით: ა) ელექტრონული კურსი, რაც გულისხმობს დისტანციურ სწავლებას; ბ) საკლასო მეცადინეობა –ტრენერის თანდასწრებით მეცადინეობა ლექციის, სემინარისა და სხვა ფორმატში; გ) მასტერკლასი – შესაბამისი დარგის პროფესიონალის მიერ გამოცდილების გაზიარება ლექციის, სემინარისა და სხვა ფორმატში; დ) სწავლა კეთებით –პრაქტიკაზე ორიენტირებული სწავლება.[19]

პროფესიული განვითარების ელექტრონული სისტემა

ვინაიდან საჯარო სამსახურის შესახებ საქართველოს კანონის შესაბამისად საჯარო დაწესებულებებმა თავიანთი ორგანიზაციის ფარგლებში უნდა განახორციელონ თანამშრომელთა პროფესიული განვითარების მართვა, e-HRMS სისტემაში პროფესიული განვითარების ახალი მოდულის დაინერგა.

პროფესიული განვითარების მოდულის მეშვეობით ორგანიზაციას შეუძლია თანამშრომელთა პროფესიული განვითარების წლიური გეგმების შედგენა, სწავლების საჭიროებების აღრიცხვა და მიღწეული შედეგების ადმინისტრირება. შესაბამისად, ადამიანური რესურსების მენეჯერს და ხელმძღვანელ პირს მუდმივად აქვთ ინფორმაცია თანამშრომლის პროფესიულ განვითარებაზე – თუ რა დაიგეგმა და რეალურად რისი განხორციელება მოხერხდა კონკრეტული წლის ფარგლებში, რის საფუძველზეც შესაძლებელი იქნება გარკვეული ანალიზის გაკეთება. ამავდროულად, თავად თანამშრომელს ექნება წვდომა მისივე პროფესიული განვითარების გეგმასა და შედეგებზე.

იმისათვის, რომ ეს მიდგომა და პროცესი e-HRMS სისტემაში სრულყოფილად ყოფილიყო რეალიზებული და მართვადი, სისტემაში განისაზღვრა სამუშაოს ორი ძირითადი გარემო:

1. e-HRMS სისტემის ძირითადი მოდული ანუ HR მენეჯერების სამუშაო გარემო.
2. Self-Service მოდულის ნაწილი – რომელიც თავისთავად მოიცავს თანამშრომლისა და მენეჯერის როლებს.

პროფესიული განვითარების მოდულის მომხმარებლები არიან:

- HR თანამშრომელი, რომელიც eHRMS სისტემაში ახორციელებს პროფესიული განვითარების წლიური გეგმების (როგორც ინდივიდუალური, ასევე ჯამური) მართვასა და ადმინისტრირებას, ასევე თანამშრომელთა პროფესიული სწავლების შედეგების აღრიცხვას;
- თანამშრომელი, რომელიც Self-Service გარემოში ხედავს თავისივე პროფესიული განვითარების წლიურ გეგმას, საშუალება აქვს, აღრიცხოს გავლილი ტრენინგისა და კურსების ინფორმაცია და ასევე დააფიქსიროს დაგეგმილი გეგმის ფარგლებში გავ-

[19] „პროფესიული საჯარო მოხელის პროფესიული განვითარების საჭიროებების განსაზღვრის წესის, პროფესიული განვითარების სტანდარტისა და წესის დამტკიცების შესახებ“ საქართველოს მთავრობის 242-ე დადგენილება, მუხლი 5.

ლილი სწავლების თაობაზე პირადი შეფასება, შეავსოს ე.წ. კმაყოფილების კითხვარი (Satisfaction Survey).

- მენეჯერი, რომელსაც გააჩნია ხედვა დაქვემდებარებულ თანამშრომლებზე და ახორციელებს მათი პროფესიული საჭიროებების აღრიცხვას მიღებული შეფასების შედეგების საფუძველზე. ამავდროულად, აქვს ინფორმაცია თავისივე პროფესიული განვითარების გეგმაზე (ასეთის არსებობის შემთხვევაში).

საჯარო სამსახურის ბიურო, რომელსაც გააჩნია ხედვა ორგანიზაციების ჯამურ პროფესიულ გეგმებსა და მიღწეულ შედეგებზე.[20]

საქმისწარმოების სისტემები

ელექტრონული მმართველობის ფარგლებში განსაკუთრებული ადგილი უკავია დოკუმენტბრუნვის ელექტრონულ სისტემებს, რომლებითაც ჩანაცვლდა საჯარო დაწესებულებებში მიმდინარე შიდა ტრადიციული პროცესები, რაც მატერიალური ფორმით საქმის წარმოებას უკავშირდებოდა.

„სახაზინო (საბიუჯეტო) დაწესებულებებში ელექტრონული მმართველობის დანერგვის შესახებ“ საქართველოს პრეზიდენტის 2011 წლის 7 ნოემბრის №698 ბრძანებულებით დაიწყო სახაზინო (საბიუჯეტო) დაწესებულებებში ადამიანური რესურსის მართვისა და საქმისწარმოების ავტომატიზებული სისტემის სტანდარტების დანერგვის პროცესი, ხოლო საქართველოს მთავრობის მიერ 2012 წლის 21 თებერვლის №64 დადგენილებით[21] განისაზღვრა სახაზინო (საბიუჯეტო) დაწესებულებებში საქმისწარმოების ავტომატიზებული სისტემის მინიმალური სტანდარტი. აღნიშნული სამართლებრივი აქტების საფუძველზე დოკუმენტბრუნვის პროცესის გამარტივების, დაჩქარების, მისი ხარისხის გაუმჯობესების მიზნით შემუშავებულ იქნა დოკუმენტბრუნვის ერთიანი ელექტრონული სისტემები.

არსებული მდგომარეობით, საქართველოში არ არსებობს საერთო დოკუმენტბრუნვის ერთიანი ელექტრონული სისტემა და დაწესებულებები ძირითადად იყენებენ სამ დამოუკიდებელ ავტომატიზებულ პროგრამას, ესენია:

1. საქართველოს იუსტიციის სამინისტროს სსიპ – საჯარო რეესტრის სააგენტოს დოკუმენტბრუნვის ერთიან ელექტრონულ სისტემა (დესი);
2. საქართველოს შინაგან საქმეთა სამინისტროს ელექტრონული დოკუმენტბრუნვის სისტემა (eFlow);

---

[20] „სამუშაოს შესრულების შეფასების გზამკვლევი“ , ია წულაია და თეიკო ბოკუჩავა, სსიპ – საჯარო სამსახურის ბიურო, 2020.

[21] „სახაზინო (საბიუჯეტო) დაწესებულებებში საქმისწარმოების ავტომატიზებული სისტემის მინიმალური სტანდარტის დამტკიცების შესახებ“ საქართველოს მთავრობის 2012 წლის 21 თებერვლის №64 დადგენილება, იხ. https://matsne.gov.ge/document/view/1595719?publication=0

3. საქართველოს ფინანსთა სამინისტროს სსიპ – საფინანსო-ანალიტიკური სამსახურის საქმისწარმოების ელექტრონული სისტემა (eDocument);

აღნიშნული სისტემების ფუნქციონირების შედეგად საჯარო დაწესებულებებში ყველა სახის კორესპონდენცია, მათ შორის მოქალაქეთა განცხადებები, ელექტრონული ფორმით წარმოებს, რაც ამარტივებს პროცესებს როგორც შიდა ორგანიზაციულ დონეზე, ასევე მესამე პირებთან ურთიერთობისას. ამასთან, დოკუმენტბრუნვის ერთიანი ელექტრონული სისტემის ფუნქციონირება ხელს უწყობს საჯარო სამსახურში ეკონომიურობისა და ეფექტიანობის პრინციპების პრაქტიკულად დანერგვას.

შესრულებული სამუშაოს შეფასების ელექტრონული სისტემა

რა არის შესრულებული სამუშაოს შეფასება?

შესრულებული სამუშაოს შეფასება მნიშვნელოვანი ინსტრუმენტია ორგანიზაციის განვითარების, კონკურენტუნარიანობის გაზრდის, ფუნქციონირების ეფექტიანობის ამაღლებისა და ორგანიზაციული კულტურის, კლიმატის დახვეწისთვის. შესრულებული სამუშაოს შეფასება გულისხმობს თანამშრომლის წვლილის გაზომვას ორგანიზაციული მიზნების მიღწევის თვალსაზრისით, რასაც გავლენა აქვს სამ მნიშვნელოვან – დაწესებულების, სტრუქტურული ერთეულისა და ინდივიდუალურ დონეზე. შესრულებული სამუშაოს შეფასების მთავარი დანიშნულებაა თანამშრომლის ძლიერი მხარეების გამოკვეთა, დაწესებულების სასარგებლოდ მათი გამოყენება, თავის მხრივ, მოტივაციის ამაღლება, წახალისების ხელშეწყობა, ასევე, გასავითარებელი მიმართულებების იდენტიფიცირება და როგორც პიროვნული, ისე პროფესიული კომპეტენციების გაუმჯობესების ხელშეწყობა.[22]

შეფასების პროცესი

შესრულებული სამუშაოს შეფასების განხორციელებისთვის არსებითია შეფასების მეთოდის, პროცედურების, ვადების, მონაწილე პირების, შედეგების გასაჩივრების მექანიზმებისა და დაწესებულების სპეციფიკიდან და საჭიროებიდან გამომდინარე, სხვა შესაბამისი ასპექტების განსაზღვრა.

შეფასების პროცესის მნიშვნელოვანი ნაწილია შეფასების გასაუბრება, რომელიც კონსტრუქციული და ტრანსფორმაციული უკუკავშირის ტექნიკების გამოყენებით აჯამებს თანამშრომლის მიერ შესრულებულ სამუშაოს, გამოკვეთს იმ ღირებულებებს, კომპეტენციებს, ქმედებებს, რომლებმაც პოზიტიური გავლენა იქონია სამუშაოს შედეგზე. ასევე, ყურადღებას ამახვილებს იმ ქცევებზე და პიროვნულ თუ პროფესიულ მახასიათებლებზე, რომლებიც

[22] „სამუშაოს შესრულების შეფასების გზამკვლევი“, პრაქტიკული სახელმძღვანელო, სსიპ – საჯარო სამსახურის ბიურო, 2020.

საჭიროებს განვითარებას, უკეთესი შედეგის მისაღწევად, რაციონალური თვითშეფასების შენარჩუნებისთვის, მოტივაციის ამაღლებისა და სამუშაოთი კმაყოფილებისთვის.

შეფასების პროცესის ელექტრონულად განხორციელების მნიშვნელობა

შეფასების პროცესი საკმაოდ კომპლექსურია და შინაარსობრივ თუ პროცედურულ დონეზე აქტიურ ჩართულობას საჭიროებს როგორც ადამიანური რესურსების მართვის, ისე მოხელეებისა და მათი მენეჯერების მხრიდან, რათა სწორად განისაზღვროს მოლოდინები შესასრულებელ სამუშაოსთან დაკავშირებით, ასევე, გაიწეროს შეფასების კრიტერიუმები, ქულათა განმარტებები, შეფასება დაეფუძნოს ობიექტურ მაჩვენებლებს და არა პიროვნულ დამოკიდებულებებს, დროულად მიეწოდოს უკუკავშირი ქცევის კორექციისა და სამუშაო პროცესის ეფექტიანობის გაზრდის მიზნით. გასათვალისწინებელია, რომ აღნიშნულ პროცესში, შეფასების ობიექტურობის გაზრდისა და მოხელეთა უფლებების დაცვის მიზნით, დგება გარკვეული დოკუმენტები, მაგალითად, ოქმები, შეფასების კრიტერიუმების, მათი აღწერილობების, ქულათა განმარტებების გაცნობისა და შეფასების წესით გათვალისწინებული სხვა მასალა, რომელიც, ცხადია, ადმინისტრირების მიმართულებით დამატებით რესურსსა და დროს მოითხოვს.

ზემოაღნიშნულიდან გამომდინარე, დამატებითი ადამიანური, დროითი და მატერიალური რესურსის დაზოგვის მიზნით, მნიშვნელოვანია, რომ შეფასების პროცესი განხორციელდეს ელექტრონულად და არსებობდეს ისეთი პლატფორმა, რომელშიც გათვალისწინებული იქნება შეფასების წესით დადგენილი ნიუანსები და შესაძლებელი იქნება შეფასების ელექტრონულად მართვა.

საქართველოს საჯარო სამსახურში მოხელეთა შეფასების საკითხებს „საჯარო სამსახურის შესახებ“ საქართველოს კანონი არეგულირებს. აღნიშნული კანონის ქვემდებარე აქტით, საქართველოს მთავრობის 2017 წლის 28 აპრილის N220 დადგენილებით დამტკიცებული „პროფესიული საჯარო მოხელის შეფასების წესი და პირობები“ უფრო დეტალურად ადგენს შეფასებასთან დაკავშირებულ საკითხებს.

აღსანიშნავია, რომ შეფასების წესი მკაფიოდ განსაზღვრავს შეფასების მთელი რიგი პროცედურების ელექტრონულად განხორციელების შესაძლებლობას. საჯარო დაწესებულების ადამიანური რესურსების მართვაზე პასუხისმგებელ პირს შეფასების დაწყებამდე ყველა საჭირო ინფორმაცია ელექტრონულად შეჰყავს პროგრამაში და შეფასების შედეგებსაც ელექტრონულად ასახავს. ასევე, შესაფასებელ მოხელესაც შეუძლია, მათ შორის, ელექტრონულად, წარადგინოს შეფასების პროცესში შექმნილი ძირითადი და დამატებითი დოკუმენტები, გააკეთოს კომენტარები, მენეჯერსაც შეუძლია ელექტრონულად დაგეგმოს შეფასების ინტერვიუ და უკუკავშირი მოხელეს დისტანციურ ფორმატში მიაწოდოს.

ამდენად, შეფასების პროცესის ელექტრონულად განხორციელება მხარდაჭერილია საკანონმდებლო დონეზე.

შეფასების ელექტრონული სისტემა

თავის მხრივ, მნიშვნელოვან ამოცანას წარმოადგენს ისეთი უნიფიცირებული ელექტრონული სისტემის არსებობა, რომელიც, საჯარო დაწესებულებების საქმიანობის სფეროს სპეციფიკის გათვალისწინებით, შესაძლებელს გახდის საკუთრივ, დაწესებულების შეფასების წესით განსაზღვრული ასპექტების პროგრამულად ასახვას, შეფასების პროცესის ელექტრონულად ადმინისტრირებას და პროგრამაში ადამიანური რესურსების მართვის ერთეულის, მოხელეებისა და მენეჯერების საქმიანობას მოქნილად, კოორდინირებულად და შედეგიანად.

აღნიშნული ამოცანა მსგავსი ელექტრონული პლატფორმის შექმნის ნაწილში შესრულებულია და ადამიანური რესურსების მართვის ავტომატიზებულ სისტემაში (e-HRMS) ჩაშენებულია შეფასების მოდული, რომელიც მაქსიმალურად მორგებულია სხვადასხვა საჯარო დაწესებულების სპეციფიკაზე და თითქმის სრულყოფილად მოიცავს ყველა იმ ძირითად ასპექტს, რომელიც საქართველოს კანონმდებლობით არის დადგენილი და ასევე, ითვალისწინებს იმ ნიუანსებს, რომლებიც პოტენციურად შესაძლებელია განსაზღვრული იყოს თითოეული დაწესებულების ინდივიდუალური შეფასების წესით. საგულისხმოა, რომ შეფასების მოდულით შეუძლიათ ისარგებლონ არა მხოლოდ იმ საჯარო დაწესებულებებმა, რომლებშიც მოხელეები არიან დასაქმებულნი, არამედ ყველა იმ ორგანიზაციამ, რომლებშიც დანერგილია ადამიანური რესურსების მართვის ავტომატიზებული სისტემა (e-HRMS).

შეფასების მოდული აერთიანებს როგორც შეფასების პროცესის ადმინისტრირების გარემოს, ისე მომხმარებლის, ე.წ „self-service“ (თანამშრომლის და მენეჯერის როლები) გარემოს. შეფასების პროცესის ადმინისტრირების გარემოში დაწესებულების ადამიანური რესურსების მართვის საკითხებზე პასუხისმგებელ პირს შეუძლია შეფასების პროცესის ინიციირება, შეფასების მეთოდის განსაზღვრა, შესაფასებელი კომპონენტების გაწერა, შეფასების საწყისი და საბოლოო თარიღების, ასევე, შუალედური შეფასების პერიოდის განსაზღვრა და სხვ.

მომხმარებლის გარემოში შესაძლებელია მიზნების/ფუნქციების/კომპეტენციების დამატება, წარმატების ინდიკატორის განსაზღვრა, შეფასების კრიტერიუმების, ქულების განმარტებების ასახვა, რასაც მენეჯერის დასტური და თანამშრომლის თანხმობა სჭირდება.

მენეჯერის როლიდან შესაძლებელია შუალედური შეფასების (ასეთის არსებობის შემთხვევაში) ადმინისტრირება პერიოდის, განხილული საკითხების, უკუკავშირის შედეგებისა და ქულის მითითებით. საბოლოო შეფასების შემთხვევაში მიეთითება მიღწეული შედეგი, შეფასების ქულა და მენეჯერის არგუმენტები.

მნიშვნელოვანია აღნიშნულ მოდულში **თვითშეფასების** განხორციელების შესაძლებლობა. მოხელეს შეუძლია პროგრამულად მიუთითოს მიღწეული შედეგი და თვითშეფასების ქულა.

შეფასების მოდულის მეშვეობით, შესაძლებელია შეფასების საბოლოო ქულის **გასაჩივრება**, შესაბამისი კომენტარის მითითებით და გასაჩივრების შედეგის აღნიშვნით.

მოდულში არსებობს მოკლე ჩანართი **გამოსაცდელ ვადაში მყოფი** მოხელეების შეფასებისთვის.

ამ ეტაპზე საჯარო დაწესებულებებს შეფასების პროცესის პროგრამულად განხორციელების ხელშეწყობისათვის განესაზღვრათ სატესტო პერიოდი, რა დროსაც ადამიანური რესურსების მართვაზე პასუხისმგებელი პირები უპირველეს ყოვლისა, თავად ცდილობენ პროგრამაში მუშაობის უნარების გაუმჯობესებას და მოხელეებსა და მენეჯერებსაც ეხმარებიან, ადვილად ადაპტირდნენ მომხმარებლის გარემოში.

ზოგიერთი დაწესებულება უკვე წარმატებით და სრული დატვირთვით იყენებს შეფასების მოდულს, დაწესებულებების ნაწილი პარალელურად საცდელ რეჟიმში ახორციელებს ელექტრონულ შეფასებას და ძირითად პროცესს კვლავ მატერიალურად წარმართავს.

დიდი ალბათობით, 2022 წლიდან საჯარო დაწესებულებების უმრავლესობა შეძლებს შეფასების სრული პროცესის ელექტრონულად განხორციელებას, რაც მნიშვნელოვნად დაზოგავს ადამიანურ და ადმინისტრაციულ რესურსს, ამასთან, გაამარტივებს და მოქნილს გახდის შეფასების პროცესს.

მომხმარებლებთან კომუნიკაცია და უკუკავშირის ელექტრონული სისტემები

ვებგვერდები

თანამედროვე ორგანიზაცია – როგორც კერძო, ასევე საჯარო სტრუქტურა – წარმოუდგენელია ვებგვერდისა და სხვა დამხმარე ონლაინ პლატფორმების გარეშე. ვებგვერდს რამდენიმე ფუნქცია აკისრია, რომელიც აუცილებლად უნდა გამოიყენოთ როგორც ორგანიზაციის საქმიანობის გასაშუქებლად, ასევე თქვენი საქმიანობის ადრესატების სასარგებლოდ: ეს არის ერთდროულად როგორც თქვენი ორგანიზაციის სავიზიტო ბარათი, ასევე მომხმარებლებისათვის ხელმისაწვდომი უკუკავშირის არხი.

ვებგვერდის მეშვეობით მოქალაქეს ან მომხმარებელს უნდა შეეძლოს ყოველგვარი ინფორმაციის მოძიება, რომელსაც იგი თქვენს ოფისში ფიზიკურად მოსვლის შემთხვევაში მიიღებდა. ასევე, მომხმარებელს უნდა შეეძლოს ვებგვერდის მეშვეობით მიიღოს ყველა (ან თითქმის ყველა) ის მომსახურება, რომელსაც თქვენი ორგანიზაცია უწევს მოქალაქეებს თავისი უფლებამოსილების ფარგლებში.

გაითვალისწინეთ, თუ, მაგალითად, მომსახურების მისაღებად საჭიროა ხელმოწერილი დოკუმენტის წარდგენა, საქართველოს კანონი „ელექტრონული დოკუმენტისა და ელექტ-

რონული სანდო მომსახურების შესახებ“[23] გაძლევთ საშუალებას, რომ სრულად დისტანციურად გაუწიოთ მომსახურება მომხმარებლებს, თუკი თქვენი უწყებისათვის უფლებამოსილების მინიჭებისა და მომსახურების მოწესრიგების შესახებ ნორმატიულ აქტში სპეციალურად არ არის ამის აკრძალვა გათვალისწინებული.

დისტანციური მომსახურების გასაწევად ან გასამართად მნიშვნელოვანი ფაქტორია როგორც ორგანიზაციის შიდა ბიზნესპროცესების გამართულობა, ასევე ტექნიკური მზადყოფნა და შესაბამისი რესურსების გამოყოფა – როგორც ადამიანური, ასევე ფინანსური. შესაბამისად, ხელმძღვანელი ან პასუხისმგებელი პირი მზად უნდა იყოს იმისთვის, რომ შესაბამისი მომსახურების გამართვას საფუძვლიანი და დეტალური დაგეგმვა და დროითი რესურსი დაჭირდება.

ძირითადი ინფორმაცია, რომელიც აუცილებლად უნდა იყოს გამოქვეყნებული ვებგვერდზე:

- ინფორმაცია თქვენი ორგანიზაციის სტრუქტურის შესახებ ხელმძღვანელობისა და მმართველი თანამდებობის პირების ჩათვლით;
- ორგანიზაციის მისამართი, საკონტაქტო ტელეფონი და ელფოსტის მისამართი უკუკავშირისათვის;
- ორგანიზაციის/უწყების საქმიანობის სფერო და უფლებამოსილება;
- სერვისები და მომსახურება, რომელსაც გაუწევთ მოქალაქეებსა თუ მომხმარებლებს;
- ახალი ამბები უწყების ყოველდღიური საქმიანობის გარშემო;
- ყველა დოკუმენტი, პუბლიკაციები, წლიური ანგარიშები და სხვა სახის მასალა (მათ შორის, აუდიო და ვიდეომასალაც), რომელსაც აქვეყნებთ უწყების საქმიანობიდან გამომდინარე.
- კონფიდენციალურობის პოლიტიკა – პერსონალურ მონაცემთა დაცვის სპეციალური დოკუმენტი.

ვებგვერდების გარდა არსებობს სხვა დამხმარე ონლაინ პლატფორმებიც, ცნობილი, როგორც სოციალური მედიის ინსტრუმენტები. ეს არის, უპირველეს ყოვლისა, საქართველოში პოპულარული Facebook, ასევე საერთაშორისო მასშტაბებით ძალზე წარმატებული Twitter. გარკვეულ შემთხვევებში, შესაძლოა, თქვენს უწყებას ასევე გამოადგეს LinkedIn – სპეციალურად შექმნილი პროფესიული სოციალური ქსელი საქმიანი ურთიერთობებისათვის. თქვენი უწყების სპეციფიკიდან გამომდინარე, შეარჩიეთ შესაბამისი პლატფორმა (მაგალითად, Facebook) და დაარეგისტრირეთ უწყების პროფილური გვერდი მომხმარებლებთან უფრო მჭიდრო და სწრაფი კომუნიკაციის მიზნით. საერთაშორისო პარტნიორებთან ურთიერთობების გასაღრმავებლად, ახალი ამბებისა და, ზოგადად, თქვენს სფეროში მიმდინარე სიახლეების გასაზიარებლად და გასავრცელებლად შეგიძლიათ გამოიყენოთ Twitter.

[23] https://matsne.gov.ge/document/view/3654557?publication=1

აუცილებლად გაითვალისწინეთ, რომ ვებგვერდის და სოციალური ქსელების სამართავად დაგჭირდებათ შესაბამისი ადამიანური რესურსი, რაც თქვენ, როგორც მენეჯერმა, უნდა გამოყოთ – დაავალოთ არსებულ კადრებს გარკვეული ფუნქციებისა და ამოცანების შესრულება, ან სპეციალურად გამოყოფილი კადრით (კადრებით) დააკომპლექტოთ შტატი.

როგორც წესი, უკვე ყველა სახელმწიფო უწყებას აქვს საკუთარი ვებგვერდი, თუმცა მათი ანალიზი აჩვენებს, რომ ბევრი მათგანი საჭიროებს განახლებას როგორც ფუნქციური, ასევე შინაარსობრივი თვალსაზრისით. მაგალითად, ბევრ გვერდი მხოლოდ ქართულ ენაზეა და რეკომენდებულია, დამზადდეს ინგლისურენოვანი ვერსიებიც, რის შემდეგაც თანაბარი სიხშირით და მნიშვნელობით გამოქვეყნდება ინფორმაცია ორივე ენაზე. ასევე სასურველია, განახლებები სისტემატური იყოს, იმგვარად, რომ თქვენი უწყების მომხმარებლები დაუბრკოლებლად გაეცნონ მიმდინარე პროცესებს და, დაინტერესების შემთხვევაში, ჰქონდეთ სრული ინფორმაციის მიღების შესაძლებლობა.

ვებგვერდის დამზადება შეგიძლიათ როგორც საკუთარი ძალებით – თუ თქვენს უწყებაში ამისათვის შესაბამისი რესურსის გამოყოფას შეძლებთ, ან დაუკვეთოთ სხვა კერძო კომპანიას თუ საჯარო ორგანიზაციას. ვებგვერდის დაკვეთისას და დამზადებისას აუცილებლად გაითვალისწინეთ ის, რომ დღესდღეობით ელექტრონულ სისტემებს და პორტალებს არანაკლებ მნიშვნელოვანი დაცვა სჭირდებათ, ვიდრე რეალურ საოფისე სივრცეებს და შენობებს. საამისოდ წინასწარ უნდა დაიგეგმოს და განისაზღვროს შიდა ორგანიზაციული ქსელური და სერვერული ინფრასტრუქტურის დაცვა, ასევე გასათვალისწინებელია, რომ უნდა შეარჩიოთ სანდო კომპანია-მომწოდებელი ვებგვერდის ჰოსტინგისათვის. თვით ვებგვერდს აუცილებლად უნდა ჰქონდეს უსაფრთხოების SSL-სერტიფიკატი და სხვა. აუცილებლად გაითვალისწინეთ, რომ საჯარო სამსახურში, სახელმწიფო უწყებებში შექმნილი ყველა ვებგვერდი და პორტალი აუცილებლად უნდა იყოს განთავსებული სპეციალურად სახელმწიფო უწყებებისათვის გამოყოფილი დაბოლოების მქონე დომენურ სახელზე – gov.ge. ამით თქვენ უზრუნველყოფთ როგორც ვებგვერდზე განთავსებული ინფორმაციის სანდოობას, ასევე თქვენი ორგანიზაციის იმიჯის გაუმჯობესებას.

ვებგვერდები გამოიყენება არა მხოლოდ თქვენი უწყებისა და საქმიანობის შესახებ ინფორმაციის გავრცელების, არამედ ასევე მომხმარებლებისგან (მოქალაქეებისგან) უკუკავშირის მიღების მიზნით. თანამედროვე სამყაროში პრიორიტეტი ენიჭება ბიზნესპროცესების ავტომატიზაციას, მომსახურების დაჩქარებას, უხერხული ბიუროკრატიული პროცედურების გაუქმებასა და დროის დაზოგვას – აქ, უპირველეს ყოვლისა, მომხმარებლის დროის დაზოგვა იგულისხმება. შესაბამისად, თქვენი ინტერესიცაა, რომ მომხმარებლებს მაქსიმალურად გაუადვილოთ როგორც ინფორმაციის, ასევე მომსახურების მიღება. აღნიშნულს მხოლოდ იმ შემთხვევაში მიაღწევთ, თუ სწორად წარმართავთ მომხმარებლებთან უკუკავშირს და, მაგალითად, თქვენს ვებგვერდზე გამოქვეყნებულ სატელეფონო ნომერზე ან ელფოსტის

მისამართზე შემოსულ კითხვებსა და მოთხოვნებს დროულად დაამუშავებთ და უპასუხებთ.

დღეს არავისთვის აღარაა სიახლე ის, რომ ელფოსტაზე შემოსული მოთხოვნა არაფრით განსხვავდება იმავე სტანდარტული, ტრადიციული წერილისგან და ამ მოთხოვნაზეც ვრცელდება საქართველოს კანონმდებლობით დადგენილი ოფიციალური პასუხის გაცემის ვადები (ხშირ შემთხვევაში ეს 10 სამუშაო დღეა).

და ბოლოს, გაითვალისწინეთ, რომ კანონმდებლობის მოთხოვნების შესაბამისად, ვებგვერდზე აუცილებლად უნდა იყოს განთავსებული პერსონალურ მონაცემთა დაცვის პოლიტიკის დოკუმენტი – ეს დოკუმენტი უნდა აღწერდეს იმ შემთხვევებს, თუ როგორ ხდება თქვენი ორგანიზაციის მიერ ვებგვერდზე შემოსული და ან რეგისტრირებული მომხმარებლების მონაცემთა დაცვა.

დოკუმენტში ასახული უნდა იყოს:

- რა სახის მონაცემების შეგროვება ხდება
- რა მიზნებისთვის ხდება მონაცემების დამუშავება
- ხდება თუ არა აღნიშნული მონაცემების გაზიარება მესამე პირებისათვის
- როგორ ხდება მონაცემთა შენახვა და უსაფრთხოების რა ზომებია დაცული
- რა უფლებები აქვს მომხმარებელს ყოველივე ზემოაღნიშნულთან მიმართებით
- სხვა ინფორმაცია, რომელსაც თქვენ მიიჩნევთ საჭიროდ

ყოველივე ზემოაღნიშნულის დანერგვისა და გამართვისათვის საჭიროა შესაბამისი ტექნოლოგიური და ინფორმაციული ცოდნა და მომზადება. არასაკმარისმა ადამიანურმა რესურსებმა შეიძლება ჯერ მომსახურების დონის დაცემა და, შედეგად, მომხმარებლის უკმაყოფილება გამოიწვიოს.

ინფორმაციული ტექნოლოგიების (IT) მართვა

ინფორმაციული ტექნოლოგიების (IT) მართვა მიზნად ისახავს, დაწესებულებას თავისი ყოველდღიური საქმიანობის განხორციელებაში ტექნოლოგიების გამოყენებით დაეხმაროს. ინფორმაციული ტექნოლოგიების მართვა ფეხდაფეხ უნდა მისდევდეს უწყების/ორგანიზაციის სტრატეგიას და მისი მიზნების მიღწევისკენ უნდა იყოს მიმართული. დღეისთვის თითქმის ყველა სფერო ინფორმაციულ ტექნოლოგიებზეა დამოკიდებული. ის, თუ რამდენად სწორედ არის ინფორმაციული ტექნოლოგიები დანერგილი ორგანიზაციაში, ხშირ შემთხვევაში დიდწილად განსაზღვრავს მის ეფექტურობას, ეფექტიანობას და საქმისწარმოების მაღალ ხარისხს. ინფორმაციული ტექნოლოგიების სწრაფი განვითარება ხელს უწყობს ძირითადი საქმიანობის უფრო ხარისხიანად წარმართვას, თუმცა, მეორე მხრივ, აჩენს კიბერუსაფრთხოებასთან დაკავშირებულ დამატებით საშიშროებებსა და რისკებს.

IT-ის მართვა იმდენად დიდი სფეროა, მისი განხილვა მცირე დოკუმენტის ფარგლებში შეუძლებელია, ამიტომ მიმოვიხილავთ იმ მინიმალურ ინფორმაციას, რაც IT-ის მართვის შესახებ უნდა ვიცოდეთ.

იმისთვის, რომ ორგანიზაციამ უკეთ მართოს თავისი საქმიანობა და გამოიყენოს ინფორმაციული ტექნოლოგიები, მას შეიძლება დასჭირდეს სასერვერო ინფრასტრუქტურა, ქსელური ინფრასტრუქტურა, მართვის ინფორმაციული სისტემები და სხვა. სასერვერო ინფრასტრუქტურის მოწყობა, ისევე როგორც მართვის ინფორმაციული სისტემის შეძენა ან საკუთარი ძალებით შექმნა დიდ დანახარჯს მოითხოვს, თუმცა შესაძლებელია სასერვერო ინფრასტრუქტურის დაქირავება მსგავსი მომსახურების მქონე კომპანიებისაგან და ყოველთვიურად გამოყენებული ინფრასტრუქტურული სიმძლავრის შესაბამისი მომსახურების თანხის გადახდა.

დღეს საკუთარი ძალებით მართვის ინფორმაციული სისტემის შექმნა გართულებულია, რადგან ამ საქმიანობას სჭირდება მაღალი კვალიფიკაციის ბიზნესანალიტიკოსების გუნდი, რომლის წევრებმაც უნდა დასახონ ამოცანა და დეტალურად აღწერონ სისტემის ფუნქციები. ამოცანის დასახვის შემდგომ პროცესში ერთვება პროგრამისტების გუნდი, რომელმაც უნდა შეასრულოს ტექნიკური სამუშაოები და შექმნას მართვის ინფორმაციული სისტემა. ისეთი უწყებისთვის/ორგანიზაციისთვის, რომლის პირდაპირი საქმიანობა არ არის პროგრამული უზრუნველყოფის შექმნა, ძალიან ძნელია ამ პროფესიის თანამშრომლების დაქირავება და მათთვის კონკურენტუნარიანი ხელფასის გადახდა. ამიტომ პროგრამული უზრუნველყოფის შექმნის საჭიროების შემთხვევაში აჯობებს, შეირჩეს ისეთი კომპანია, რომელიც ნიშანდობლივად ამ საქმითაა დაკავებული და შესაბამისი გამოცდილებაც გააჩნია, ჰყავს საჭირო რაოდენობის სპეციალისტები და შესწევს ძალა, მოთხოვნების მიხედვით შექმნას მართვის ინფორმაციული სისტემა.

IT ინფრასტრუქტურის ერთ-ერთი უმნიშვნელოვანესი კომპონენტია ელექტრონული ფოსტის მართვის სერვერი (Mail Server), რომელიც პასუხს აგებს თანამშრომლების ელფოსტის ფუნქციონირებაზე. იმისათვის, რომ Mail Server-მა გამართულად იმუშაოს, აუცილებელია მის ადმინისტრირებაზე იზრუნოს შესაბამისი კვალიფიკაციის სპეციალისტმა, რომელიც შეიძლება თავად ორგანიზაციაში მუშაობდეს სრულ ან ნახევარ განაკვეთზე, ანდა იყოს იმ კომპანიის წარმომადგენელი, რომელიც თქვენ IT მხარდაჭერას გიწევთ. დღეისთვის ელფოსტით იგზავნება სხვადასხვა ვირუსი, მავნე კოდის შემცველი ფაილები, რომელთა გახსნასაც შეიძლება მოჰყვეს კომპიუტერზე უცხო პირის მიერ კონტროლის დაწესება, ასევე ხშირია ინტერნეტთაღლითების მიერ გამოგზავნილი წერილები, ამიტომ აუცილებელია, რომ Mail Server მაქსიმალურად იყოს დაცული ავტომატური საშუალებებით, რათა არასასურველი წერილების მიღება თავიდან ავიცილოთ.

ინციდენტების მართვის სისტემები

ამ თავში განვიხილავთ ინციდენტებთან მოპყრობის მნიშვნელობას, მათზე რეაგირების სხვადასხვა მეთოდს და რეაგირებისას აუცილებლად გასათვალისწინებელ საკითხებს.

ინციდენტი არასასურველი მოვლენაა, რომელიც ორგანიზაციის ან მასზე დამოკიდებული სხვა ორგანიზაციების სტანდარტული ოპერაციების ნაწილად არ მიიჩნევა და რომელმაც შეიძლება გამოიწვიოს ორგანიზაციის საქმიანობის, მომსახურების ან ფუნქციების შეწყვეტა ან შეფერხება. ინციდენტების მაგალითებია: ორგანიზაციის რომელიმე სისტემაზე კიბერშეტევა, ხანძარი, ინფორმაციის ან სხვა რაიმე აქტივის ქურდობა, არასწორად დაგეგმილი მომსახურების პროცედურების გამო ინფორმაციის ან მომხმარებლის დაკარგვა და სხვა.

ნებისმიერი სახელმწიფო უწყება თუ კერძო ორგანიზაცია უფლებამოსილების განხორციელებისას, მომსახურების ან პროდუქციის მიწოდებისას, ცდილობს, შეფერხებები თავიდან აიცილოს და საკუთარი საქმიანობა ხარისხიანად და ეფექტურად წარმართოს. ისიც ცნობილია, რომ არავინაა დაზღვეული ინციდენტისგან. ამიტომ ნებისმიერი ორგანიზაციის ფუნქციონირება ინციდენტების ეფექტიანი მართვის გარეშე შეუძლებელია.

ინციდენტების მართვა არის პროცესი, რომლის დროსაც ხდება იმ საშიშროებებისა და რისკების იდენტიფიცირება, რომლებიც შეიძლება დაემუქროს ორგანიზაციის საქმიანობას, მათი შემდგომი ანალიზი და გამოსწორების გზების მოძიება, რათა თავიდან იქნეს აცილებული მსგავსი ინციდენტის შემდგომი განმეორება. ძალიან იშვიათად, მაგრამ შესაძლოა ერთმა ინციდენტმა არა მხოლოდ ხელი შეუშალოს, არამედ ზოგ შემთხვევაში საერთოდ გააჩეროს ორგანიზაციისათვის სასიცოცხლოდ მნიშვნელოვანი პროცესები და მომსახურებები.

მაგალითისათვის განვიხილოთ ორგანიზაცია, რომელიც მომხმარებლებს ემსახურება „Front Office“-ით, რაც ნიშნავს, რომ ამ უწყების ოპერატორები სხვადასხვა სერვისის ფარგლებში იღებენ განცხადებებს როგორც ფიზიკური ასევე იურიდიული პირებისაგან, რომლებიც შემდგომ იგზავნება სხვა, შესაბამისი სახელმწიფო უწყების მართვის ინფორმაციულ სისტემაში. დავუშვათ, ორგანიზაცია N1-ის მომსახურებებს გასცემს „Front Office“-ის ოპერატორების შესაბამისი ჯგუფი, ხოლო ორგანიზაცია N2-ის მომსახურებებს – ოპერატორების სხვა ჯგუფი. შესაძლოა, ორგანიზაცია N1-ის რომელიმე მომსახურების ფარგლებში ოპერატორის მიერ განაცხადის შევსებისას დაფიქსირდეს ხარვეზი და, მაგალითად, 10 წუთის განმავლობაში მოქალაქისათვის მომსახურების გაწევა ვერ მოხერხდეს. ამ ინციდენტის თაობაზე ინფორმაცია უნდა აისახოს ინციდენტების მართვის სისტემაში და შესაბამისმა თანამშრომელმა მასზე დაყრდნობით უნდა აღმოფხვრას პრობლემა.

მსგავსი ინციდენტი შეიძლება მოხდეს ორგანიზაცია N2-ის მომსახურების მიწოდებისასაც. რადგან მოქალაქე ოპერატორთან იცდის, აუცილებელია, დროულად აღდგეს შეფერხებუ-

ლი პროცესის ნორმალური ფუნქციონირება, ხოლო შემდგომ აღმოიფხვრას ინციდენტის გამომწვევი მიზეზები. დროული რეაგირებისათვის კი საჭიროა, შესაბამისი მოვალეობები სწორ პოზიციებზე/თანამშრომლებზე იყოს გადანაწილებული. როლების სწორად განაწილების შედეგად შესაბამისმა თანამშრომლებმა იციან, როგორი ტიპის ინციდენტი რომელ თანამშრომელს ან თანამშრომელთა ჯგუფს უნდა მიაწოდოს განსახილველად და ამიტომ რეაგირების პროცესი ოპტიმალური სქემით ხორციელდება.

იმ შემთხვევაში, თუ ინფორმაცია ერთდროულად რამდენიმე ინციდენტის თაობაზე დაფიქსირდა, მნიშვნელოვანია, თანამშრომელმა, რომელიც ვალდებულია მათზე რეაგირება მოახდინოს, იცოდეს, რომელი ინციდენტია პრიორიტეტული. შესაბამისად, აჯობებს, თუ წინასწარ მოხდება იმ პარამეტრებისა და ზოგადი მიდგომების განსაზღვრა, როგორ უნდა მიენიჭოს პრიორიტეტი ამა თუ იმ ინციდენტს.

ჩვენ განვიხილეთ ორი სხვადასხვა უწყების მომსახურებების შემთხვევა, როდესაც ორივეგან ხდება ინციდენტები. ინციდენტების მართვის სისტემის დანერგვისას შესაძლებელია სხვადასხვა მიდგომის გამოყენება. მაგალითად, შეიქმნას ინციდენტების მართვის ერთიანი სისტემა, სადაც ინფორმაცია თავს მოიყრის ორივე უწყების ინციდენტების შესახებ. მეორე მიდგომის თანახმად, შესაძლებელია შეიქმნას ინციდენტების მართვის განაწილებული ორი სისტემა, რომლებშიც განცალკევებულად აღირიცხება ორგანიზაცია N1-ის და ორგანიზაცია N2-ის ინციდენტები. პირველი მიდგომა საერთო ანგარიშგების წარმოების, ამას გარდა, მთლიანი ორგანიზაციის ჭრილში ინციდენტების მართვის წარმადობისა და სხვა მაჩვენებლების კონტროლის საშუალებას იძლევა.

მეორე მიდგომა საერთო ანგარიშგების შესაძლებლობას არ მოგვცემს, მაგრამ, სამაგიეროდ, შემცირდება ინციდენტის თაობაზე ინფორმაციის საბოლოო შემსრულებლისთვის მიწოდების დრო, რაც, ჯამში, ინციდენტებზე რეაგირების დროს შეამცირებს. აუცილებელია, ხელმძღვანელობამ შეაფასოს ორგანიზაციისა და მომსახურებების სპეციფიკა და საწყის ეტაპზევე შეარჩიოს ინციდენტების მართვის სისტემისადმი სწორი მიდგომა.

საერთოდ, ინციდენტის მიერ შეწყვეტილი პროცესის აღდგენის შემდგომ, ამ ინციდენტის გამომწვევ მიზეზებს ბოლომდე შეისწავლიან და, საჭიროების შემთხვევაში, აღმოფხვრიან, რათა მსგავსი რამ აღარ გამეორდეს. ამ პროცესს **პრობლემების მართვა** ეწოდება. რიგ შემთხვევებში პრობლემების მართვისას აუცილებელი ხდება კომპლექსური სამუშაოების ჩატარება, რაც თავისთავად გულისხმობს ახალი პროექტის ინიციირებას. ახალი პროექტი კი შედგება რამდენიმე ან ბევრი ამოცანისგან, რომელთა შესრულებაზე, წარმადობასა და ხარისხზე კონტროლი აუცილებელია მისი წარმატებით დასრულებისა და საწარმოო გარემოში გაშვებისათვის, რაზეც შემდეგ თავში ვისაუბრებთ.

დროის / დავალებების მართვის სისტემები

დროისა და დავალებების მართვა ყოველდღიური სამუშაოს უმნიშვნელოვანესი ნაწილია. შესაბამისად, ამ თავში განვიხილავთ, როგორ უნდა ვმართოთ და დროში გავანაწილოთ დავალებები თუ რესურსები.

დავალების მართვა არის პროცესი, რომელიც მიმდინარეობს დავალების აქტიური ციკლის განმავლობაში და მოიცავს დაგეგმვის, შესრულების, ტესტირების, მონიტორინგისა და ანგარიშგების ეტაპებს. დავალებების მართვა ეხმარება თითოეულ თანამშრომელს და თანამშრომელთა გუნდს, ეფექტიანად და ოპტიმალურად გაანაწილონ სამუშაო დრო, აკონტროლონ მათ მიერ შესასრულებელი დავალებები და საბოლოო ჯამში მიაღწიონ დასახულ მიზანს.

დავალებების მართვა გაცილებით ეფექტიანია, თუ მათ აღრიცხავენ სპეციალიზებული პროგრამული უზრუნველყოფის მეშვეობით, როგორებიცაა საქმისწარმოების სისტემები ან პროექტების მართვის სისტემები. მსგავსი სისტემები საშუალებას იძლევა, დავალებების ჭრილში ოპტიმალურად გავანაწილოთ თანამშრომლები და სხვა საჭირო რესურსები, დავსახოთ შუალედური შედეგები და ინდიკატორები. მათი გამოყენებით მარტივია თანამშრომელთა დატვირთვის კონტროლი, რათა სამუშაოები სწორად გადანაწილდეს. შესაძლებელია პროექტის განხორციელების ვადისა და თვითღირებულების გამოთვლა იმ მონაცემებზე დაყრდნობით, რომლებიც წინასწარ არის ცნობილი. მსგავსი პროგრამული უზრუნველყოფა, როგორც წესი, აღჭურვილია ანგარიშგების ფუნქციით, მაგალითად, რომელ დავალებას ვინ ასრულებს, რამდენი ხანია განსაზღვრული თითოეული დავალების შესრულებისათვის, რა ანაზღაურებაა გათვალისწინებული თითოეული თანამშრომლისათვის, როგორია დავალებების შესრულების თანმიმდევრობა, ურთიერთდამოკიდებულება და სხვა.

დავალებების აღწერისას და შესაბამისი პასუხისმგებელი პირების განსაზღვრისას აუცილებელია პრიორიტეტების მითითება. დროის ერთსა და იმავე მონაკვეთში პარალელური დავალებების არსებობისას აუცილებელია, პირველად შესრულდეს დავალება, რომელსაც უფრო მაღალი პრიორიტეტი აქვს მინიჭებული. პრიორიტეტების ცოდნა მნიშვნელოვანია ყველა თანამშრომლისთვის, რათა ორგანიზაცია ერთსულოვნად ისწრაფოდეს დასახული მიზნისაკენ.

დავალებების ეტაპობრივად შესრულების პროცესში შესაძლებელია იმის განსაზღვრა, თუ დაგეგმილთან შედარებით რა გადახრებით შესრულდა ესა თუ ის დავალება. როგორი იყო დავალებების შესრულების დაგეგმილი ვადა და რეალურად რა დროში შესრულდა ისინი – ამ ყოველივეს შედარებითი ანალიზი შეგვიძლია ანალიტიკურ ანგარიშგებაში ვნახოთ. ანგარიშგებაში იმის ნახვაც შეიძლება, პროექტის ფარგლებში რომელმა თანამშრომელმა რამდენ საათს იმუშავა და რა ანაზღაურება გამოიმუშავა, როგორია თითოეული თანამშრომლის დატვირთვა და შეფარდება განაკვეთურ და ზეგანაკვეთურ სამუშაოებს შორის.

აუცილებელი და მნიშვნელოვანი ფუნქციაა შესაბამის თანამშრომელთან შეტყობინებების გაგზავნაც, როდესაც რაიმე აქტივობის დასრულების ვადა ახლოვდება. დავალებებს შეიძლება მიენიჭოს სხვადასხვა სტატუსი, მაგალითად: „შესრულების პროცესშია“, „დასრულებულია“, „შეწყვეტილია“ და სხვა. ამ სტატუსისა და მისი გამომწვევი მიზეზის მიხედვით, ხელმძღვანელობას სხვადასხვა გადაწყვეტილების მიღება შეუძლია.

რამდენიმე მნიშვნელოვანი რჩევა მენეჯერებისათვის, რომლებიც დავალებებს ანაწილებენ:

დავალების განსაზღვრა
გაიაზრეთ და გადაწყვიტეთ, რომ ამოცანა სხვა თანამშრომელზე დელეგირებისთვის შესაფერისია.

განსაზღვრეთ შესაბამისი თანამშრომელი ან გუნდი
რა მიზნით აპირებთ ამ დავალების დელეგირებას? რა შედეგს ელით დავალების შესრულებისას?

შეაფასეთ შესაძლებლობა
შეაფასეთ, შეუძლია თუ არა ცალკეულ თანამშრომელს ან თანამშრომელთა ჯგუფს ამ დავალების შესრულება. ესმით თუ არა დავალების არსი.

მიზნები
აუცილებელია, თანამშრომლებს ავუხსნათ დავალების მიზანი, რატომ შეარჩიეს კონკრეტულად ისინი ამ დავალების შესასრულებლად, საერთო სქემაში რა დანიშნულება აქვს ამ დავალებას და მასზე პასუხისმგებელ თანამშრომელს.

შედეგები
თანამშრომელმა უნდა იცოდეს, რა შედეგი უნდა მიიღოს დავალების შესრულების შემდეგ. უნდა დავრწმუნდეთ, რომ მას შედეგებზე სწორი წარმოდგენა აქვს. ამისათვის შესაძლოა გავეცნოთ მის ხედვასაც. უნდა განვსაზღვროთ, როგორ გაიზომება შედეგი და რა იქნება მიღწევის ინდიკატორი. უნდა დავრწმუნდეთ, რომ თანამშრომელმა იცის, როგორ გაიზომება მის მიერ დავალების შესრულების ეფექტურობა.

საჭირო რესურსების განსაზღვრა
დასაწყისშივე, ერთობლივად უნდა მოხდეს საჭირო რესურსების იდენტიფიცირება. რესურსებში იგულისხმება თანამშრომლები, შენობა, აღჭურვილობა, ბიუჯეტი, მასალები და ამ დავალებასთან დაკავშირებული სხვა აქტივობები და მომსახურება.

ვადების შეთანხმება
აუცილებელია დავალების ან პროექტის თითოეული ეტაპისათვის დასრულების ვადებისა და შუალედური შედეგების ვადების განსაზღვრა.

მხარდაჭერა და კომუნიკაცია
ძალიან მნიშვნელოვანია ინფორმაციის დროული გაზიარება დაინტერესებული მხარეებისა და თანამშრომლებისათვის. ინფორმაციის დროული მიწოდება ხელს უწყობს დავალების წარმატებით და დროულად შესრულებას.

უკუგება და მიღებული შედეგი

აუცილებელია, თანამშრომელმა იცოდეს, მიაღწია თუ არა მიზანს დავალების ფარგლებში, როგორ შეფასდა მის მიერ განხორციელებული სამუშაო. თუ დავალების შესრულების პროცესში პრობლემამ იჩინა თავი, აუცილებელია ამ პრობლემის და მისი გამომწვევი მიზეზების განხილვა, რათა შემდგომში გაუმჯობესდეს თანამშრომლის პროდუქტიულობა.

მენეჯერისთვის საჭირო ონლაინ ინსტრუმენტები ყოველდღიური საქმიანობისთვის

2020 წლის პანდემიიდან გამომდინარე, დისტანციურ სამუშაოზე გადასვლის გამო რადიკალურად შეიცვალა ყოველდღიური სამუშაო განრიგი და თანამშრომლების ჩვევები, მენეჯერებს დასჭირდათ ახალი სამუშაო ინსტრუმენტებისა და ონლაინ პლატფორმების გამოყენება. გარდა იმისა, რომ უფრო დიდი ყურადღება უნდა დაეთმოს სწორ კომუნიკაციას სამსახურის გარეთ – სხვა უწყებებთან, მომხმარებლებთან, მესამე პირებთან; ასევე დიდი მნიშვნელობა მიენიჭა როგორც უწყებრივ კომუნიკაციას (თანამშრომლებს შორის, თანამშრომლებსა და მენეჯმენტს შორის) და, თავისთავად, ტექნიკური ინფრასტრუქტურის გამართულობას.

დისტანციური მუშაობის პირობებში განსაკუთრებით მნიშვნელოვანია, უწყების თანამშრომლებმა ეფექტიანად განაგრძონ მუშაობა და საერთო საკითხების გარშემო კოორდინაცია მოახერხონ. თანამედროვე ონლაინსერვისები იძლევა იმის საშუალებას, რომ რამდენიმე თანამშრომელმა დოკუმენტებზე ერთდროულად მუშაობა შეძლოს, ჰქონდეთ საერთო საცავი ამ დოკუმენტებისათვის.

უპირველეს ყოვლისა, სასურველია, ყველა თანამშრომელს ჰქონდეს წვდომა უწყების დოკუმენტთბრუნვის პროგრამებსა და დაარქივებულ დოკუმენტებზე – ამისათვის ტექნიკურმა სამსახურმა უნდა უზრუნველყოს შესაბამისი წვდომის მოწესრიგება, რიგ შემთხვევებში თანამშრომლების პირად კომპიუტერებზე VPN სერვისის გამართვა. საჭიროების შემთხვევაში შესაძლებელია, დისტანციური მუშაობის პერიოდის განმავლობაში თანამშრომლებს ნება დართოთ, წაიღონ სამსახურის კომპიუტერები და სახლიდან იმუშაონ.

პირადი და კორპორაციული ელფოსტა

ტრადიციულად, სავიზიტო ბარათზე საკონტაქტო მონაცემებთან ერთად ელფოსტის მისამართიც იწერება. სავიზიტო ბარათის ერთ-ერთი უმნიშვნელოვანესი დანიშნულება როგორც საკუთარი თავის წარდგენა, ასევე თქვენი საქმიანობისა და თქვენი ორგანიზაციის დანარჩენებისთვის გაცნობაა. აქედან გამომდინარე, უაღრესად მნიშვნელოვანია, რომ საკონტაქტო მონაცემები სწორად და სრულად იყოს მითითებული და ექვემდებარებოდეს გარკვეულ წესებსა თუ ნორმებს. ერთ-ერთი ასეთი დაუწერელი ნორმა დღევანდელ სამყაროში ისაა, რომ სამსახურებრივი საქმიანობისათვის თანამდებობის პირებს (განსაკუთრებით კი საჯარო სამსახურში მომუშავეებს) ბარათზე თავიანთი ორგანიზაციის ოფიციალური ელფოსტის მისამართი უნდა ჰქონდეთ მითითებული.

უმნიშვნელოვანესია, თქვენი ელფოსტის მისამართი ემთხვეოდეს თქვენი ვებგვერდის მისამართს. როგორც წესი, ორგანიზაციების უმეტესობაში ამას ტექნიკური მხარდაჭერის სამსახური უზრუნველყოფს, თუმცა არის შემთხვევები, როდესაც ორგანიზაციას შეიძლება რამდენიმე ვებგვერდი ან პორტალი ჰქონდეს. ასეთ შემთხვევაში, ელფოსტისთვის გამოიყენეთ ისეთი მისამართი, რომელზეც თქვენი ძირითადი საქმიანობის ვებგვერდია განთავსებული.

ასევე გაითვალისწინეთ, რომ მომხმარებლებს არავითარ შემთხვევაში არ უნდა მისწეროთ თქვენი პირადი ელფოსტის მისამართით; საქმიანი ურთიერთობისას სანდოობის გარანტი მხოლოდ თქვენი უწყების ოფიციალური ელფოსტის მისამართია.

აღსანიშნავია, რომ „სახელმწიფო ენის შესახებ“ საქართველოს ორგანული კანონის შესაბამისად, სახელმწიფო და მუნიციპალიტეტის ორგანოებს შორის ურთიერთობა და მიმოწერა სახელმწიფო ენაზე ხორციელდება და აღნიშნულის გათვალისწინება უნდა მოხდეს ელფოსტით კომუნიკაციის დროსაც. ასევე, აუცილებელია ელექტრონული ფოსტით გაგზავნილი თითოეული წერილის დასათაურება.

რაც შეეხება ვებგვერდს, როგორც ზემოთ აღვნიშნეთ, შესაბამისი მისამართი მომხმარებლებში სანდოობის შეგრძნებას იწვევს, დადებითად აისახება ორგანიზაციის იმიჯზე, მაგრამ არსებობს ერთი მნიშვნელოვანი ფაქტორი: მონაცემთა დაცვა. აქ იგულისხმება როგორც ვებგვერდის დაცვა კიბერშეტევებისაგან, ასევე ელფოსტით გაგზავნილი და მიღებული ფაილების დაცვა, ინფორმაციის კონფიდენციალურობა.

არავითარ შემთხვევაში არ გამოიყენოთ სხვადასხვა პოპულარული უფასო სერვისები სამსახურებრივი მიმოწერისათვის. Gmail, Yahoo და სხვა სერვისები ერთი შეხედვით შეიძლება სანდო და დაცულ სერვისებად მიგაჩნდეთ, მაგრამ საქმიანი მიმოწერის დროს არასაკმარისი სანდოობა აქვს. თქვენი სამსახურებრივი მისამართიდან გაგზავნილი წერილი ნამდვილად მიუთითებს იმაზე, რომ პირადად თქვენ აგზავნით მას. სხვადასხვა უფასო სერვისებზე შესაძლებელია როგორც მისამართის გაყალბება, ასევე მსგავსი სახელისა და გვარის დარქმევა, ამ გზით კი თაღლითობის ალბათობა ბევრად მაღალია.

გარდა აღნიშნულისა, ცალკე უნდა მიმოვიხილოთ ისეთი უფასო გვერდები, როგორებიცაა Yandex, Mail.ru და სხვა მსგავსი რუსული საფოსტო სერვისები. ზემოხსენებული თაღლითობის ალბათობის გარდა, არსებობს ორი დამატებითი რისკი: უპირველესად თქვენი, როგორც საჯარო მოხელის რეპუტაციის რისკი; მეორე კი, ბევრად უფრო საგულისხმო და მნიშვნელოვანი ფაქტორია ის, რომ თქვენ მიერ ასეთი ელფოსტის სერვისებით გაგზავნილ და მიღებულ დოკუმენტებზე წვდომას მიიღებენ უცხო ქვეყნების სპეცსამსახურები. ცნობილია, რომ რუსეთის მთავრობა სხვადასხვა საკანონმდებლო შეზღუდვებითა და სანქციებით აიძულებს კერძო კომპანიებს (მათ შორის, საერთაშორისო კომპანიებსაც), სრულად გადასცენ ამ კომპანიების ხელში მყოფი ინფორმაცია რუსეთის სახელმწიფო უსაფრთხოების ორგანოებს. შესაბამისად, თქვენი უწყების ბიუჯეტი, საშტატო განრიგი, წლიური ანგარიში, ასევე ბევრად უფრო მოსაფრთხილებელი ან საიდუმლო ინფორმაცია პირდაპირ ხელში უვარდება მტრულად განწყობილი სახელმწიფოს სპეცსამსახურს.

სახელმწიფო უწყებების თანამშრომლების მიერ სამსახურებრივი მოვალეობის შესრულებისას პირადი ელფოსტის გამოყენების მიზეზი ხშირად ისაა, რომ მათ ორგანიზაციაში Mail Server-ი ისე არ არის გამართული, რომ თანამშრომელმა მისი კომფორტულად მოხმარება შეძლოს, ან მას უბრალოდ უჭირს ორი ელფოსტის გამოყენება და მხოლოდ

პირად მიმოწერას ადევნებს თვალყურს. თუმცა, როგორც უკვე აღინიშნა, სულერთია, რა მიზეზის გამო, მიუღებელია კორპორაციული ელფოსტის არგამოყენება. ეს აზიანებს როგორც თავად სახელმწიფო უწყების, ისე ქვეყნის იმიჯსაც. ამას გარდა, როდესაც საჯარო მოსამსახურე იყენებს ისეთ Mail Server-ების მომსახურებას, როგორებიცაა mail.ru, rambler.ru, Yandex.ru და სხვა, ეს ნიშნავს, რომ მისი ელფოსტის მეშვეობით გადაცემულ-გადმოცემული ინფორმაცია შესაძლებელია მარტივად ჩავარდეს დიდი საფრთხის მომტანი ჯგუფების ხელში. ამიტომ, აუცილებელია დავიმახსოვროთ, რომ სამსახურებრივი მიზნებისათვის უაღრესად მნიშვნელოვანია, გამოვიყენოთ მხოლოდ კორპორაციული ელფოსტა.

იგივე ეხება სხვადასხვა პროგრამულ უზრუნველყოფასაც, რომლებიც შეიძლება თქვენი უწყების სისტემების მუშაობისათვის დაგჭირდეთ. ესენია: ანტივირუსები, დაარქივების პროგრამები და ა.შ. გაითვალისწინეთ უსაფრთხოებისა და სხვა რისკები მსგავსი პროგრამული უზრუნველყოფის, მომსახურების ან სერვისის შესყიდვისას.

აღნიშნული რისკების დასაზღვევად დაგეგმილია ერთიანი მიდგომის შემუშავება და გარკვეული სახის სერვისებზე წვდომის შეზღუდვა ყველა სახელმწიფო უწყების სამსახურებრივი ქსელებიდან. სასურველია, რომ თქვენც, როგორც მენეჯერს, უწყების შიგნით შემუშავებული გქონდეთ გარკვეული წესი და ტექნიკური საშუალებებით დაბლოკოთ წვდომა აღნიშნულ სერვისებზე.

დოკუმენტებთან მუშაობა

როგორც უკვე აღვნიშნეთ, განსაკუთრებით მნიშვნელოვანია, რომ უწყების თანამშრომლებს სამუშაო პროცესის განმავლობაში ეფექტური კომუნიკაცია ჰქონდეთ. თავისთავად, ეს გულისხმობს ხშირ კავშირს ტელეფონითა და ელფოსტით, თუმცა არსებობს ბევრი სხვადასხვა საშუალება, რომ ონლაინ ინსტრუმენტების გამოყენებით თანამშრომლებს დოკუმენტებზე ერთდროული მუშაობა შეეძლოთ.

როგორც თქვენთვის ცნობილია, სხვადასხვა დონის დოკუმენტების, წერილების, პრეზენტაციებისა თუ ანგარიშების მომზადების დროს საჭიროა არა მარტო ერთი თანამშრომლის მონაწილეობა, არამედ სხვადასხვა სამმართველოსა თუ დეპარტამენტის თანამშრომლების პერიოდული კომენტარები, თანხმობა ან საბოლოო დასტური ამა თუ იმ ტექსტზე ან ტექსტის ნაწილზე.

შესაბამისად, საჭიროა დოკუმენტების ვერსიათა კონტროლი, მკაფიოდ განსაზღვრული ვადები – თუ ვინ როდის უნდა მოგცეთ უკუკავშირი ამა თუ იმ დოკუმენტზე და სხვა მნიშვნელოვანი დეტალები. დოკუმენტების გაზიარების ტრადიციული (ელფოსტით) გზის გარდა, არსებობს დოკუმენტებთან *ერთდროული* მუშაობისათვის შექმნილი ე.წ. „ქლაუდ“

(cloud) სერვისები – როდესაც ონლაინ შენახულ დოკუმენტზე რამდენიმე ადამიანს ერთდროულად აქვს წვდომა, სადაც მათ შეუძლიათ რეალურ დროში შეიტანონ დოკუმენტებში ცვლილებები, ნახონ თანამშრომლების წვლილი და იქვე განიხილონ შესაძლო ღია საკითხები.

აღნიშნულ სერვისებს უკვე მრავალი წელია იყენებენ კერძო კომპანიები და ეს განსაკუთრებით ხელსაყრელია დისტანციური მუშაობის დროს, ასევე იმ შემთხვევებში, როდესაც უწყებას ან ორგანიზაციას რამდენიმე ადგილას აქვს ოფისი ან ფილიალი.

ასეთი სერვისების ვრცლად ჩამოთვლა შორს წაგვიყვანს, ამიტომ მაგალითად მხოლოდ რამდენიმე პოპულარულ სერვისს მოვიყვანთ:

Google Drive – ერთიანი სივრცე დოკუმენტების შესანახად, თითოეულ მომხმარებელს აქვს გამოყოფილი სივრცე და შეუძლია მოიწვიოს თანამშრომლები დოკუმენტებზე ერთობლივად სამუშაოდ. არსებობს როგორც უფასო ვერსია შედარებით მცირე მოცულობის მეხსიერებით, ასევე ფასიანი ვერსიების ფართო არჩევანი.
დრაივის სამი ძირითადი შემადგენელი ნაწილია: Docs – იგივეა რაც ჩვეულებრივი დოკუმენტების რედაქტორი; Sheets – ცხრილების რედაქტორი რიცხვითი და ფინანსური ოპერაციებისათვის; Slides – პრეზენტაციების შესაქმნელად.

Microsoft OneDrive – თქვენთვის უკვე ჩვეული საოფისე პროგრამების ონლაინსაცავი, სადაც მარტივად შეგიძლიათ იმუშაოთ იმავე პროგრამებით, რომლებიც ოფისში გაქვთ: Word, Excel, PowerPoint. აქაც არსებობს როგორც ფასიანი, ისე უფასო ვერსიები – მეხსიერების სხვადასხვა მოცულობით. ვინაიდან ეს სერვისი ეკუთვნის Microsoft-ს, ის ასევე ინტეგრირებულია ყველა თანამედროვე Windows ოპერაციულ სისტემაში, რათა მოსახერხებელი იყოს მისი გამოყენება.

Dropbox – არანაკლებ პოპულარული და საკმაოდ ფართოდ გავრცელებული სერვისი იმავე ფუნქციებით, როგორებიც ზემოხსენებულ ორ სერვისს აქვს.
ერთ-ერთი ყველაზე მთავარი და ძალზე მოსახერხებელი ფუნქცია, რაც ზოგადად „ქლაუდ“ სერვისებს გააჩნიათ და მათ შორის, ზემოხსენებულ სამივე სერვისსაც, არის დოკუმენტების სინქრონიზაცია სხვადასხვა კომპიუტერებსა თუ მობილურებში. ეს ნიშნავს, რომ სხვადასხვა კომპიუტერიდან შესვლის, ასევე მობილური აპლიკაციის გამოყენების შემთხვევაში ხელი ყოველთვის მიგიწვდებათ დოკუმენტის ყველაზე ახალ, ბოლო ვერსიაზე.

გთხოვთ, რომ ზემოხსენებულ სერვისებთან მუშაობის შემთხვევაშიც ისევე უნდა დაიცვათ კიბერუსაფრთხოებისა და კიბერჰიგიენის წესები, რაც სხვა დროს: რეგისტრაციისას გამოიყენეთ სამსახურებრივი ელფოსტის მისამართები, შექმენით რთული პაროლები (კომბინაციები ასოების, ციფრებისა და სიმბოლოების გამოყენებით), არ გადასცეთ პაროლები მესამე პირებს და სხვა.

ვიდეოზარები და სხვა ონლაინ ხელსაწყოები

როგორც ზემოთ უკვე ვახსენეთ, დისტანციური მუშაობის პერიოდში საჭირო გახდა მრავალი ახალი და განსხვავებული პროგრამული უზრუნველყოფის გამოყენება, რომლებიც ხელს უწყობენ თანამშრომლების კოორდინაციას და ასევე გეხმარებათ თქვენ, როგორც მენეჯერს, მართოთ ცალკეული თანამშრომლები ან თანამშრომელთა ჯგუფები.

გარდა იმისა, რასაც მენეჯერი თავის ყოველდღიურ საქმიანობაში ახორციელებს, როგორც უწყების ხელმძღვანელი პირი – უფლებამოსილების განხორციელება, ორგანიზაციის წარმომადგენლობა, გადაწყვეტილებების მიღება და სხვა, მისი ამოცანაა ასევე თანამშრომელთა მართვა, ინფორმირება ყოველდღიური სამუშაო პროცესის მიმდინარეობის თაობაზე. აღნიშნულიდან გამომდინარე, სასურველია, თქვენ, როგორც მმართველი რგოლის წარმომადგენელს, გქონდეთ ყოველდღიური თუ არა, ყოველკვირეული სისტემატური შეხვედრები თქვენს დაქვემდებარებულ თანამშრომლებთან. შესაძლოა, უწყების ზომიდან გამომდინარე, ფიზიკურად შეუძლებელი იყოს დიდი რაოდენობის თანამშრომლებთან პირისპირ შეხვედრების ყოველდღიურად გამართვა, მაგრამ ორგანიზაციის სტრუქტურული ერთეულების ხელმძღვანელებთან მაინც უნდა შეგეძლოთ სისტემატური კონტაქტი. ეს საჭიროა როგორც თქვენი ინფორმირებულობისათვის, ასევე პროცესების დასაჩქარებლად და გადაწყვეტილებების დროულად მისაღებად.

ვიდეოზარები შესაძლებლობას გაძლევთ, მარტივი და მოხერხებული გზით გადაჭრათ აღნიშნული პრობლემები დისტანციური მუშაობის პირობებში. უწყების სამუშაო სპეციფიკიდან გამომდინარე, თქვენთვის შეიძლება ყოველკვირეული ვიდეოკონფერენცია კმაროდეს, ან ყოველ დილას მოკლე, ნახევარსაათიანი სესიების ჩატარება დაგჭირდეთ. ამასთან, ცალკეულ საკითხებზე შეგიძლიათ ცალკეული შეხვედრები დანიშნოთ – ეს ყველაფერი ვიდეოზარების მეშვეობით შეგიძლიათ მოახერხოთ.

მიუხედავად იმისა, რომ აღნიშნული შესაძლებლობები ადრეც არსებობდა, ხალხი მაინც ხარჯავდა დროს ტრანსპორტში და პირად შეხვედრებს ანიჭებდა უპირატესობას. დღევანდელი პირობებიდან გამომდინარე, ადამიანების უმეტესობა უკვე მიეჩვია ონლაინსესიებს და დღეს ონლაინშეხვედრების ჩატარება ბევრად უფრო ადვილია.

ვიდეოზარებისათვის შეგიძლიათ გამოიყენოთ, მაგალითად, შემდეგი სერვისები:

Google Meet – ერთ-ერთი ყველაზე მარტივი სერვისი, არ საჭიროებს სპეციალური პროგრამული უზრუნველყოფის ინსტალაციას კომპიუტერზე. აქვს ყველა ძირითადი ფუნქცია: ეკრანის გაზიარება, მიმოწერა და ა.შ., თუმცაღა, კონკურენტებისგან განსხვავებით, არ გააჩნია სხვა დამატებითი ფუნქციები.

Zoom – ბოლო წლის განმავლობაში ძალიან პოპულარული და ძლიერი ინსტრუმენტი. გამოიყენება არა მარტო უბრალო შეხვედრების ჩასატარებლად, არამედ ლექციების, სემინარების,

კონფერენციებისთვისაც. სტანდარტული ფუნქციების გარდა, აქვს სხვადასხვა დამატებითი ფუნქცია, როგორებიცაა ხელის აწევა (მოსწავლეებისათვის), დისტანციური წვდომა ერთი მომხმარებლისათვის მეორე მომხმარებლის კომპიუტერის მართვაზე და ა.შ. საჭიროებს სპეციალური პროგრამული უზრუნველყოფის ინსტალაციას კომპიუტერზე.

Skype – ვიდეოზარებისათვის განკუთვნილი ყველასათვის კარგად ნაცნობი პროგრამაა, რომელიც უკვე დიდი ხანია, Microsoft-მა შეიძინა და რომელიც ავტომატურად ინტეგრირებულია ყველა თანამედროვე Windows ოპერაციულ სისტემაში.

ზემოხსენებული ონლაინსერვისების გამოყენება შეგიძლიათ სურვილისამებრ ან იმის მიხედვით, თუ რომელი უფრო მოსახერხებელია თქვენთვის. როგორც წესი, ყველა ორგანიზაციას ელფოსტის შემთხვევაში უკვე აქვს არჩეული გარკვეული სერვისპროვაიდერი კომპანიები, ამიტომ, საოფისე პროგრამული უზრუნველყოფის შემთხვევაში ლოგიკური იქნება, ახალი სერვისებისა და პროგრამული უზრუნველყოფის დამატებისას გაითვალისწინოთ ეს ფაქტორი და გამოიყენოთ იმ კომპანიის მომსახურება, რომელთან ურთიერთობის გამოცდილება უკვე გაქვთ. აქ საგულისხმოა თქვენი როგორც მომხმარებლის, გამოცდილება, მაგრამ არანაკლებ მნიშვნელოვანია თქვენი ტექნიკური უზრუნველყოფის სამსახურისა და თანამშრომლების გამოცდილებაც როგორც სერვისების გამართვის, ასევე მხარდაჭერის თვალსაზრისით.

ელექტრონული ხელმოწერა

ელექტრონული დოკუმენტის არსი

ელექტრონულ მმართველობაში ელექტრონულ დოკუმენტბრუნვას და ელექტრონულ ხელმოწერას ერთ-ერთი ცენტრალური ადგილი უკავია. სწორედ ელექტრონული დოკუმენტბრუნვაა ელექტრონული მმართველობის დანერგვის უმთავრესი წინაპირობა.

ჩვენთვის ცნობილი ტერმინი „ხელმოწერა“ ძალიან ძველია – დოკუმენტების შემოწმების ამოცანა უძველესი დროიდან იდგა კაცობრიობის წინაშე[24]. ადამიანების მიერ წერის ათვისებისთანავე მათი იდენტიფიცირების საშუალებად ჩამოყალიბდა სახელისა და გვარის უნიკალური მოხაზულობა, რომელსაც ფეოდალიზმის პერიოდში დაემატა შესაბამისი გვარების (ძირითადად დიდგვაროვანთა) გერბების ტვიფრებით დოკუმენტის დაბეჭდვა. ხშირად ის ხელმოწერასთან ერთად გამოიყენებოდა. ითვლებოდა, რომ ეს კომბინაცია დოკუმენტს გაყალბებისაგან მკაცრად იცავდა, თუმცა აღნიშნული მოსაზრება ისევე სადავოა, როგორც საპირისპიროს მტკიცება, რადგან იმ დროისათვის არც კრიმინალისტიკისათვის ცნობილი გრაფიკული ექსპერტიზა არსებობდა; ამგვარი დოკუმენტების სანდოობის დამტკიცება მხოლოდ მის ხელმომწერთან გადამოწმების შემდეგ შეიძლებოდა დადასტურებულიყო, შესაბამისად, არ არსებობდა არავითარი გარანტია იმისა, რომ შუა საუკუნეების ნიჭიერი თაღლითი ვერ მოახერხებდა როგორც ხელმოწერის, ასევე გერბის ტვიფრის ან შტამპის გაყალბებას.

კომპიუტერული ტექნოლოგიების განვითარებასთან ერთად მწვავედ დადგა სატელეკომუნიკაციო საშუალებებით გადაცემული ინფორმაციის ავთენტურობის პრობლემა. პირველ ეტაპზე ციფრული დოკუმენტის გაყალბება გაცილებით ადვილი იყო. მაგალითად, თავდაპირველ ეტაპზე ელექტრონული ფოსტით მიღებულ ხელშეკრულებას ან სხვა დოკუმენტს დაბეჭდავდნენ, ხელს მოაწერდნენ (დამატებით ბეჭდით დამოწმების ჩათვლით), შემდეგ კი ასკანირებდნენ და დოკუმენტს გრაფიკულ გამოსახულებად აქცევდნენ, საბოლოოდ, ციფრულ სკანირებულ ვერსიას მეორე მხარეს უბრუნებდნენ. შესაბამისად, ტექნოლოგიები ახალ, ელექტრონული ხელმოწერის ეტაპზე გადავიდა.

დღეისათვის ციფრული ელექტრონული ხელმოწერა შედეგია გარკვეული კრიპტოგრაფიული ალგორითმების მუშაობისა, რომელსაც დასაწყისში მიეწოდება ორი აუცილებელი ელემენტი: მონაცემთა ერთობლიობის ჰეში, რომელიც აღწერას ექვემდებარება და ხელმოწერის მფლობელის საიდუმლო გასაღები[25].

პრაქტიკაში ციფრული ელექტრონული ხელმოწერისათვის ძირითადად იყენებენ ე.წ. „ასიმეტრიული კრიპტოგრაფიის“ მეთოდს, რომელიც აქტიურად გამოიყენება „ბლოკჩეინ ტექნოლოგიებში“. გარდა ამისა, არსებობს ციფრული ხელმოწერის უფრო რთული ვარიანტებიც. თანამედროვე ინფორმაციულ ტექნოლოგიებში გამოიყენება ისეთი რთული სისტე-

[24] ციხილოვი ა.. ბლოკჩეინი. პრინციპები და საფუძვლები, თბ., 2020, გვ. 45

[25] იქვე, გვ. 45.

მებიც, როგორებიცაა მაგალითად, ე.წ. „ბრმა ხელმოწერა“[26], „რგოლური ხელმოწერა“[27], „მულტიხელმოწერა“[28] და ა.შ.

გარდა ამისა, პრობლემები წარმოიქმნება კომუნიკაციის ავთენტურობასთან დაკავშირებითაც. ორივე საკითხი ელექტრონული ხელმოწერის საშუალებით შეიძლება გადაიჭრას[29]. იმისათვის, რომ ელექტრონული საშუალებების გამოყენებით დადებული ხელშეკრულება წერილობითი ფორმის ხელშეკრულებას გაუთანაბრდეს, აუცილებელია მისი ხელმოწერა. ნათელია, ელექტრონული დოკუმენტის თავისებურებებიდან გამომდინარე, შეუძლებელია მისი ხელმოწერა ჩვეულებრივი მნიშვნელობით, ის ელექტრონული საშუალებებითაც უნდა მოხდეს. ელექტრონული ხელმოწერა მხოლოდ ციფრული ხელმოწერა არ არის, ეს უფრო ფართო ცნებაა. ელექტრონული ხელმოწერის მრავალი განმარტება არსებობს, მაგრამ ყველა მათგანს აერთიანებს გარკვეული ინფორმაცია, რომელიც ელექტრონული დოკუმენტის ნაწილია, ან მასთან ლოგიკურადაა დაკავშირებული და აუცილებელია მისი ავთენტიფიკაციისათვის[30].

ელექტრონული დოკუმენტისა და ელექტრონული ხელმოწერის დეფინიციას, სახეებსა და მისი გამოყენების წესებს ითვალისწინებს 2017 წლის 21 აპრილის საქართველოს კანონი „ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ“. აღნიშნულმა კანონმა ჩაანაცვლა მანამდე მოქმედი 2008 წლის 26 მარტის კანონი „ელექტრონული ხელმოწერისა და ელექტრონული დოკუმენტის შესახებ“.

---

26 „ბრმა ხელმოწერა“ – ციფრულ ტექნოლოგიებში უწოდებენ ისეთი ალგორითმის გამოყენებას, როდესაც სისტემის ერთი წევრი შიფრავს შეტყობინებას და უგზავნის მას მეორე წევრს, რომელიც წარმოადგენს სანდო კვანძს სისტემაში. სანდო წევრი ბრმად სვამს თავის ხელმოწერას დაშიფრულ შეტყობინებაზე, ისე რომ მისი შინაარსი არ იცის. ამის შემდეგ შეტყობინება გამგზავნს უბრუნდება. ეს პროცესი მარტივ ენაზე რომ ავხსნათ, დაახლოებით იმას ჰგავს, როცა სანდო წევრი იღებს დალუქულ კონვერტს, შეტყობინების დაშიფრული ფურცლით და ასლგადამტანი ქაღალდით. მიმღების ხელმოწერა ავტომატურად აისახება ასლგადამტან ქაღალდზეც. როცა გამგზავნი კონვერტს იბრუნებს და ხსნის, მასში კონვერტზე ხელმოწერილ ქაღალდთან ერთად შიდა დოკუმენტის ასლზე ხელმოწერაც დახვდება. „ბრმა ხელმოწერას“ სხვაგვარად „სამტკიცეს ნულოვანი გამჟღავნებითაც“ უწოდებენ.

27 „რგოლური ხელმოწერა“ ჯერ კიდევ მე-18 საუკუნეში იყო ცნობილი ბრიტანელი და მოგვიანებით ამერიკელი სამხედროებისთვის. როდესაც ისინი სხვადასხვა სახის საჩივრებს უგზავნიდნენ ზემდგომ ოფიცრებს, ტექსტის გარშემო რგოლურად, წრიულად აწერდნენ ხელს, რათა არ გამჟღავნებულიყო, ვინ იყო ინიციატორი ანუ პირველი ხელმომწერი (ამით დასჯის ერთგვარ პრევენციას ახდენდნენ). მოგვიანებით ელექტრონული სისტემების განვითარების შედეგად შეიქმნა სპეციალური მათემატიკური ალგორითმი – საჯარო გასაღებების გარკვეული სისტემა, რომელიც სისტემის სხვა მონაწილეებთან ავტონომიურად იყო დაკავშირებული.

28 „მულტიხელმოწერა“ გამოიყენება ისეთ სიტუაციაში, როცა შესაბამისი ციფრული ხელმოწერის ალგორითმი ერთდროულად სისტემის რამდენიმე წევრის შეთანხმებით მიღებული გადაწყვეტილებით მოქმედებს. ასეთი ტიპის ხელმოწერები ძირითადად გამოიყენება ელექტრონული ანგარიშების ჯგუფური მართვისას, რომლის დროსაც შესაბამისი ტრანზაქციის ნამდვილობას რამდენიმე მონაწილე ამოწმებს.

29 ზამბახიძე თ. ელექტრონული ვაჭრობის სამართლებრივი რეგლამენტაციის საფუძვლები (პრობლემები და პერსპექტივა). ქართული სამართლის მიმოხილვა 8/2005-1/2. გვ. 125

30 იქვე, გვ, 124

კანონის მიღება მიზნად ისახავდა არსებული სამართლებრივი ბაზის ევროპული კავშირის კანონმდებლობასთან შესაბამისობას. კერძოდ, ახალ კანონში ასახულია ყველა ნოვაცია, რომელიც „ელექტრონული იდენტიფიკაციის, შიდა ბაზარზე ელექტრონულ ტრანზაქციებთან დაკავშირებული სანდო სერვისებისა და 1999/93/EC დირექტივის გაუქმების შესახებ ევროპარლამენტისა და საბჭოს 2014 წლის 23 ივლისის N910/2014 რეგულაციის“ ფარგლებში იქნა შემუშავებული[31].

ელექტრონული დოკუმენტის ცნება ჯერ კიდევ „ელექტრონული ხელმოწერისა და ელექტრონული დოკუმენტის შესახებ“ კანონში იყო განმარტებული. კერძოდ, ცნება „წერილობითი დოკუმენტი“ გულისხმობდა დოკუმენტის ორ ფორმას: ელექტრონულსა და მატერიალურს. ელექტრონული დოკუმენტი განისაზღვრებოდა როგორც ელექტრონული, ოპტიკური ანდა სხვა მსგავსი საშუალების გამოყენებით შექმნილი, გაგზავნილი, მიღებული ან შენახული წერილობითი ინფორმაცია, რომელიც ადასტურებს იურიდიული მნიშვნელობის ფაქტს ან იურიდიული მნიშვნელობის არმქონე ფაქტს; ხოლო მატერიალური დოკუმენტი – ქაღალდზე ან სხვა მატერიალურ მატარებელზე წარმოდგენილი ინფორმაცია, რომელიც ადასტურებს იურიდიული მნიშვნელობის ფაქტს ან იურიდიული მნიშვნელობის არმქონე ფაქტს[32];

ახალმა კანონმა „ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ“ გააუქმა „წერილობითი დოკუმენტის“ ცნება და დოკუმენტის ორივე სახე ცალ-ცალკე შემდეგნაირად განსაზღვრა: ა) ელექტრონული დოკუმენტი – ელექტრონული ფორმით შენახული ტექსტობრივი, ხმოვანი, ვიზუალური ან აუდიოვიზუალური ინფორმაციის ან/და მონაცემთა ერთობლიობა; ბ) მატერიალური დოკუმენტი – ქაღალდის ან სხვა მატერიალური ფორმით წარდგენილი ინფორმაციის ან/და მონაცემთა ერთობლიობა[33];

მნიშვნელოვანია ის, რომ კანონის მიხედვით ელექტრონული დოკუმენტის ყველა ეგზემპლარი ორიგინალია[34]. ელექტრონულ დოკუმენტს არ შეიძლება ჰქონდეს ელექტრონული ასლი. ელექტრონული დოკუმენტის გამოყენება შესაძლებელია ყველა შემთხვევაში, როდესაც მოითხოვება წერილობითი ფორმის მატერიალური დოკუმენტი, თუ კანონით სხვა რამ არ არის დადგენილი.

---

31 იქვე, გვ. 87

32 იხ. „ელექტრონული ხელმოწერისა და ელექტრონული დოკუმენტის შესახებ“ საქართველოს კანონის მე-2 მუხლის „ა“ პუნქტის „ა.ა“ და „ა.ბ“ ქვეპუნქტები (როგორც აღვნიშნეთ, აღნიშნული კანონი ძალადაკარგულია – ზ.გ.) https://matsne.gov.ge/ka/document/view/20866?publication=5 (ბოლო ნახვის თარიღი 23.03.2021)

33 იხ. „ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ“ საქართველოს კანონის მე-2 მუხლის „ა“ და „ბ“ პუნქტები. https://matsne.gov.ge/ka/document/view/3654557?publication=0#DOCUMENT:1; (ბოლო ნახვის თარიღი 23.03.2021)

34 იხ. „ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ“ საქართველოს კანონის მე-4 მუხლი (3.1). https://matsne.gov.ge/ka/document/view/3654557?publication=0#DOCUMENT:1; (ბოლო ნახვის თარიღი 24.03.2021)

ელექტრონული დოკუმენტის ამონაბეჭდი არის ელექტრონული დოკუმენტის ასლი და მას ელექტრონული დოკუმენტის თანაბარი იურიდიული ძალა აქვს, თუ ის ხელმოწერისთვის პასუხისმგებელი პირის ან საქართველოს კანონმდებლობით გათვალისწინებული უფლებამოსილი პირის მიერ არის დამოწმებული ან/და დადასტურებული.

მატერიალური დოკუმენტის ელექტრონულ ასლს ორიგინალის თანაბარი იურიდიული ძალა აქვს, თუ ის ხელმოწერისთვის პასუხისმგებელი პირის ან საქართველოს კანონმდებლობით გათვალისწინებული უფლებამოსილი პირის მიერ ან/და ელექტრონული შტამპით არის დამოწმებული ან/და დადასტურებული[35].

უნდა აღინიშნოს, რომ საქართველოს საჯარო სტრუქტურებიდან ელექტრონული დოკუმენტბრუნვა განსაკუთრებით განვითარებულია იუსტიციის სისტემაში. უძრავი ქონების შესახებ ამონაწერისა და ბიზნესსუბიექტის შესახებ ამონაწერის ინტერნეტით განახლების სერვისით საჯარო რეესტრის ეროვნული სააგენტოს მომხმარებლები წლებია სარგებლობენ. მაგალითად, სტატისტიკურად, გასულ წელს ელექტრონული ამონაწერის მომსახურებით 9103-მა მომხმარებელმა ისარგებლა. აღსანიშნავია, რომ ეს რიცხვი 2013 წელთან შედარებით მნიშვნელოვნადაა გაზრდილი. 2013 წელს ინტერნეტით ამონაწერი 6469-მა პირმა განაახლა[36].

საჯარო რეესტრის ეროვნული სააგენტო ბიზნესსუბიექტის შესახებ დაინტერესებულ პირებს ამონაწერის განახლებას სააგენტოს ოფიციალური ვებგვერდის www.napr.gov.ge-ისა და www.my.gov.ge-ის დახმარებით სთავაზობს. დაინტერესებულ პირს ნებისმიერ დროს შეუძლია ამონაწერის მისაღებად ვებგვერდზე განთავსებული ელექტრონული განაცხადის ფორმა შეავსოს, მომსახურების საფასური ელექტრონულად, საბანკო პლასტიკური ბარათით გადაიხადოს და ამონაწერი განსაზღვრულ ვადაში ასევე ელექტრონულად მიიღოს.

ელექტრონული ამონაწერის მზადყოფნის შესახებ მომხმარებელს სარეგისტრაციო განცხადებაში მითითებულ მობილური ტელეფონის ნომერზე მოკლე ტექსტური შეტყობინება ეგზავნება. სააგენტოს მიერ მომზადებული ამონაწერის მიღება დაინტერესებულ პირს ასევე ვებგვერდის საშუალებით შეუძლია.

აღნიშნულმა სერვისმა უდავოდ უზრუნველყო პანდემიის პერიოდში საჯარო რეესტრის საქმიანობის ეფექტურობა და მინიმუმამდე შეამცირა ასეთ ადგილებში ინფიცირების შემთხვევები.

განსაკუთრებით საინტერესოა ელექტრონული ხელმოწერის გამოყენების საკითხი თანამდებობის პირის მიერ ქონებრივი დეკლარაციის წარდგენისას. თანამდებობის პირის ქონებრივი დეკლარაციის ტექნიკურად სწორად შევსების ინსტრუქციის მე-18 მუხლში დეტალურადაა აღწერილი დეკლარაციის ჩაბარებისას კვალიფიციური ელექტრონული ხელ-

[35] იქვე, მე-4 მუხლის პ. 4.

[36] იხ. https://napr.gov.ge/p/854 (ბოლო ნახვის თარიღი 25.03.2021)

მოწერის გამოყენების პროცედურა. კერძოდ, მე-18 მუხლის მიხედვით, „თანამდებობის პირის ქონებრივი მდგომარეობის დეკლარაციის ჩაბარება შესაძლებელია მხოლოდ დეკლარაციის კვალიფიციური ელექტრონული ხელმოწერით დამოწმების შემდეგ (პ.1). ღილაკზე „დეკლარაციის ჩაბარება“ დაჭერის შედეგად, გამოდის დიალოგური ფანჯარა, ფუნქციური ღილაკებით: „დახურვა“ და „ხელმოწერა“ (პ. 2). „ხელმოწერა“ – ღილაკი აქტიურია, თუ ხელმოწერა განხორციელებული არ არის (პ. 3). „ხელმოწერა“ – ღილაკზე დაჭერის შედეგად, სისტემა უზრუნველყოფს სსიპ – სახელმწიფო სერვისების განვითარების სააგენტოს ხელმოწერის პროგრამის (GeoID) ჩატვირთვას (პ.4). ხელმოწერის წარმატებით განხორციელების შედეგად: დეკლარაციის PDF ფაილს ედება ელექტრონული ხელმოწერა (პ.5); შესაბამისი პროგრამა (GeoID) იხურება და ბლოკში „დეკლარაციის ნახვა და ხელმოწერა“ გამოდის შეტყობინება: „ხელმოწერა წარმატებით განხორციელდა“ (პ. 6).

ვფიქრობთ, რომ კვალიფიციური ელექტრონული ხელმოწერა თანდათან საჯარო სამსახურის სხვადასხვა სფეროშიც პოვებს აქტიურ გამოყენებას, რაც ერთის მხრივ გააიოლებს ბიუროკრატიას და მეორეს მხრივ დაზოგავოს ხელმომწერი მხარეების დროს.

ელექტრონული ხელმოწერა და მისი სახეები

„ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ“ საქართველოს კანონის მიღებამდე ელექტრონული ხელმოწერა განმარტებული იყო, როგორც „ნებისმიერი ელექტრონული საშუალების გამოყენებით შექმნილ მონაცემთა ერთობლიობა, რომელსაც ხელმომწერი იყენებს ელექტრონულ დოკუმენტთან მისი კავშირის აღსანიშნავად“[37]. თუმცა კანონმა ელექტრონული ხელმოწერა განმარტა, როგორც „ელექტრონულ მონაცემთა ერთობლიობა, რომელიც დაერთვის ან ლოგიკურად უკავშირდება ელექტრონულ დოკუმენტს და ელექტრონული დოკუმენტის ხელმოსაწერად გამოიყენება“[38]. გარდა ამისა, ელექტრონულ ხელმოწერასთან ერთად, შემოიტანა ელექტრონული შტამპის ცნებაც. ელექტრონული შტამბის ცნება და შინაარსი ქვემოთ ცალკე იქნება განმარტებული, თუმცა ისიც უნდა ითქვას, რომ ელექტრონული შტამპის რეგულირების ბევრი სამართლებრივი საკითხი ელექტრონულ ხელმოწერასთან ერთად განიხილება.

კანონის მთავარი სიახლეა ის, რომ მან განსაზღვრა ელექტრონული ხელმოწერისა და ელექტრონული შტამპის შემოწმების მონაცემების, ასევე მონაცემებისა და საშუალებების ცნება. კანონმა შემოიტანა ელექტრონული ხელმოწერისა და ელექტრონული შტამპის სერტიფიკატის ცნებაც.

---

37 დარჯანია თ., საქართველოს სამოქალაქო კოდექსის კომენტარი, მუხლი 69.

38 იხ. 21.042017 საქართველოს კანონი „ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ“ მე-2 მუხ. „ე“ ქვეპუნქტი.

ელექტრონული ხელმოწერის და/ან ელექტრონული შტამპის შემოწმების მონაცემები გულისხმობს მონაცემებს, რომლებიც ელექტრონული ხელმოწერის/ელექტრონული შტამპის შესამოწმებლად გამოიყენება, ხოლო მათი შექმნის მონაცემები არის უნიკალური მონაცემები, რომლებსაც ხელმომწერი და/ან შტამპის დამსმელი ელექტრონული ხელმოწერის/ელექტრონული შტამპის შესაქმნელად იყენებს. ელექტრონული ხელმოწერის/ელექტრონული შტამპის შექმნის საშუალება კი გულისხმობს პროგრამული ან/და აპარატული უზრუნველყოფის საშუალებების ერთობლიობას, რომელიც ელექტრონული ხელმოწერის/ელექტრონული შტამპის შესაქმნელად გამოიყენება.

რაც შეეხება ელექტრონული ხელმოწერის და/ან ელექტრონული შტამპის სერტიფიკატს, ის წარმოადგენს უნიკალურ ელექტრონულ დოკუმენტს, რომელიც ელექტრონული ხელმოწერის და/ან ელექტრონული შტამპის შემოწმების მონაცემებს ხელმომწერთან და/ან შტამპის დამსმელთან აკავშირებს და შეიცავს, სულ მცირე, ხელმომწერის სახელს ან/და ფსევდონიმს/შტამპის დამსმელის სრულ სახელწოდებასა და საიდენტიფიკაციო კოდს (ასეთი კოდის არსებობის შემთხვევაში).

წინათ არსებული აღიარებული შეხედულებით, ელექტრონული ხელმოწერა შეიძლება ყოფილიყო მარტივი, რომლის განხორციელებაც მარტივი საშუალებების გამოყენებით შეიძლება (მაგ., სკანირებული ხელმოწერის მიმაგრებით). ამასთან, ასეთი ხელმოწერების განხორციელების უსაფრთხოება დაბალი იყო. მისგან განასხვავებდნენ განვითარებულ ელექტრონულ ხელმოწერას, რომელიც წყვილი გასაღების გამოყენებით ხორციელდებოდა. ხელშეკრულების ელექტრონული გზით დასადებად საჭირო იყო ხელმოწერის ტექნიკურად უსაფრთხო და სამართლებრივად აღიარებული საშუალებები[39].

როგორც ზემოთაც აღვნიშნეთ, „ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ“ საქართველოს კანონმა ელექტრონულ ხელმოწერასთან ერთად შემოიტანა ახალი ცნება – ელექტრონული შტამპი. გარდა ამისა, კანონმა განსაზღვრა ელექტრონული ხელმოწერისა და ელექტრონული შტამპის განსხვავებული სახეები.

ელექტრონული ხელმოწერის ძირითად სახედ განისაზღვრა განვითარებული ელექტრონული ხელმოწერა, ხოლო მის ნაირსახეობად – კვალიფიციური ელექტრონული ხელმოწერა.

განვითარებული ელექტრონული ხელმოწერა წარმოადგენს ელექტრონული ხელმოწერის სახეს, რომელიც უნდა აკმაყოფილებდეს შემდეგ მოთხოვნებს:

ა) იგი მხოლოდ ხელმომწერთანაა დაკავშირებული;
ბ) მისი მეშვეობით ხელმომწერის დადგენაა შესაძლებელი;
გ) შექმნილია ელექტრონული ხელმოწერის შექმნის იმ მონაცემების საშუალებით, რო-

[39] ზამბახიძე თ. ელექტრონული ვაჭრობის სამართლებრივი რეგლამენტაციის საფუძვლები (პრობლემები და პერსპექტივა). ქართული სამართლის მიმოხილვა 8/2005-1/2. გვ 125-127

მელთა გამოყენებაც ხელმომწერს მტკიცე რწმუნებით, ერთპიროვნული კონტროლით შეუძლია;

დ) იგი ხელმოწერილ მონაცემებთან ისეა დაკავშირებული, რომ მათი შემდგომი ცვლილების აღმოჩენის შესაძლებლობას იძლევა.

კვალიფიციური ელექტრონული ხელმოწერა წარმოადგენს განვითარებული ელექტრონული ხელმოწერის ნაირსახეობას, რომელიც კვალიფიციური ელექტრონული ხელმოწერის შექმნის საშუალების გამოყენებით, კვალიფიციური ელექტრონული ხელმოწერის სერტიფიკატის საფუძველზეა შესრულებული. კვალიფიციური ელექტრონული სერტიფიკატი განისაზღვრება, როგორც ელექტრონული ხელმოწერის სერტიფიკატი, რომელსაც გასცემს კვალიფიციური სანდო მომსახურების მიმწოდებელი[40], რომელიც აკმაყოფილებს შემდეგ მოთხოვნებს და უნდა შეიცავდეს, სულ მცირე:

ა) ელექტრონული დამუშავებისათვის გამოსადეგ აღნიშვნას იმის თაობაზე, რომ სერტიფიკატი გაცემულია, როგორც კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის სერტიფიკატი;

ბ) მონაცემთა ერთობლიობას, რომელიც საკმარისია კვალიფიციური სანდო მომსახურების მიმწოდებლის იდენტიფიკაციისათვის: სულ მცირე, კვალიფიციური სანდო მომსახურების მიმწოდებლის დასახელებას და იმ ქვეყნის კოდს, რომელშიც ის არის რეგისტრირებული;

გ) მონაცემთა ერთობლიობას, რომელიც საკმარისია ხელმომწერის/შტამპის დამსმელის იდენტიფიკაციისათვის: სულ მცირე სახელს ან/და ფსევდონიმს/სრულ სახელწოდებასა და საიდენტიფიკაციო კოდს;

დ) კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის შემოწმების მონაცემებს, რომლებიც შეესაბამება კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის შექმნის მონაცემებს;

ე) სერტიფიკატის მოქმედების დაწყებისა და დასრულების თარიღებს;

ვ) სერტიფიკატის საიდენტიფიკაციო ნომერს, რომელიც სანდო მომსახურების მიმწოდებლისთვის უნიკალურია;

ზ) იმ ელექტრონული მომსახურების ელექტრონულ მისამართს, რომელიც შეიძლება გამოყენებულ იქნეს სერტიფიკატის მოქმედების სტატუსის გამოსათხოვად;

თ) ელექტრონული დამუშავებისათვის გამოსადეგ აღნიშვნას ელექტრონული ხელმო-

---

[40] **კვალიფიციური სანდო მომსახურების მიმწოდებელი** – პირი, რომელიც ავტორიზებულია ამ კანონის შესაბამისად და ახორციელებს ამ კანონით გათვალისწინებული ერთი ან ერთზე მეტი კვალიფიციური სანდო მომსახურების მიწოდებას (მუხ. 2, პ. „ფ“); **კვალიფიციური სანდო მომსახურება** – სანდო მომსახურება, რომლის მიზანია კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის ან დროის კვალიფიციური აღნიშვნის და მათთან დაკავშირებული კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის სერტიფიკატის შექმნა, შემოწმება, ნამდვილობის დადგენა ან/და შენახვა (მუხ. 2, პ. „უ“); https://matsne.gov.ge/ka/document/view/3654557?publication=0#DOCUMENT:1; (ბოლო ნახვის თარიღი 25.03.2021)

წერის/ელექტრონული შტამპის შექმნის მონაცემების ელექტრონული ხელმოწერის/ელექტრონული შტამპის შექმნის კვალიფიციურ საშუალებაში განთავსების თაობაზე (აღნიშნული მონაცემების ამგვარ საშუალებაში განთავსების შემთხვევაში)[41].

უნდა აღინიშნოს, რომ კვალიფიციური ელექტრონული ხელმოწერისა და კვალიფიციური ელექტრონული შტამპის მიმართ წაყენებული მოთხოვნები იდენტურია. თუმცა, სერტიფიკატის მფლობელის მოთხოვნის შემთხვევაში, შინაგანაწესით განსაზღვრულ ფარგლებში კვალიფიციური ელექტრონული ხელმოწერის ან/და კვალიფიციური ელექტრონული შტამპის სერტიფიკატი შეიძლება დამატებით მონაცემებს შეიცავდეს. კვალიფიციური სანდო მომსახურების მიმწოდებელს უფლება აქვს, დამატებითი მონაცემები შეიტანოს კვალიფიციური ელექტრონული ხელმოწერის ან/და კვალიფიციური ელექტრონული შტამპის სერტიფიკატთან დაკავშირებულ სხვა ელექტრონულ დოკუმენტში (ატრიბუტების კვალიფიციური სერტიფიკატი), რომელიც უნდა აკმაყოფილებდეს შემდეგ მოთხოვნებს:

ა) იგი უნდა შეიცავდეს მონაცემებს, რომლებითაც შესაძლებელია კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის სერტიფიკატის იდენტიფიკაცია;
ბ) უნდა ჰქონდეს კვალიფიციური სანდო მომსახურების მიმწოდებლის განვითარებული ელექტრონული ხელმოწერა/განვითარებული ელექტრონული შტამპი.

კვალიფიციურ ელექტრონულ ხელმოწერას აქვს პირადი ხელმოწერის თანაბარი იურიდიული ძალა.

კვალიფიციური ელექტრონული შტამპი იძლევა ელექტრონული დოკუმენტის მთლიანობისა და წარმომავლობის სისწორის დადასტურების შესაძლებლობას – ელექტრონული დოკუმენტის მთლიანობა და წარმომავლობა უტყუარად ითვლება, ვიდრე საწინააღმდეგო არ დამტკიცდება.

თუ ფიზიკური პირი ან კერძო სამართლის იურიდიული პირი ადმინისტრაციულ ორგანოსთან ურთიერთობისას კომუნიკაციის ელექტრონულ ფორმას აირჩევს და მის მიერ წარდგენილი დოკუმენტი ხელმოწერას ან/და შტამპს საჭიროებს, სავალდებულოა დოკუმენტზე კვალიფიციური ელექტრონული ხელმოწერის შესრულება ან/და კვალიფიციური ელექტრონული შტამპის დასმა. ეს წესი არ ვრცელდება იმ შემთხვევაზე, როდესაც საქართველოს კანონმდებლობა არ მოითხოვს დოკუმენტზე ხელმოწერას ან/და შტამპის დასმას. ადმინისტრაციული ორგანო ვალდებულია, ელექტრონულ დოკუმენტზე შეასრულოს კვალიფიციური ელექტრონული ხელმოწერა ან/და დასვას კვალიფიციური ელექტრონული შტამპი. საკმარისია ადმინისტრაციული ორგანოს მიერ ელექტრონულ დოკუმენტზე კვალიფიციური ელექტრონული შტამპის დასმა.

---

[41] იხ. „ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ“ საქართველოს კანონის მე-6 მუხლი (პ.1). https://matsne.gov.ge/ka/document/view/3654557?publication=0#DOCUMENT:1; (ბოლო ნახვის თარიღი 26.03.2021)

კვალიფიციური ელექტრონული ხელმოწერის გამოყენება სავალდებულო არ არის ადმინისტრაციული ორგანოს სტრუქტურულ ერთეულებსა/ქვედანაყოფებსა და ტერიტორიულ ორგანოებს შორის ან/და მათ ფარგლებში ურთიერთობისას. ამ შემთხვევაში გამოყენებულ ელექტრონულ დოკუმენტსა და ელექტრონულ ხელმოწერას აქვს, შესაბამისად, მატერიალური დოკუმენტისა და პირადი ხელმოწერის თანაბარი იურიდიული ძალა.

ამასთან, დაუშვებელია ადმინისტრაციული წარმოებისას და სასამართლოში სამართალწარმოებისას ელექტრონულ დოკუმენტზე უარის თქმა მხოლოდ იმ მოტივით, რომ ის ელექტრონული ფორმითაა წარდგენილი; თუმცა ეს არ გამორიცხავს ელექტრონული დოკუმენტის შესაბამის წარმოებაში მიღებაზე უარის თქმას იმ შემთხვევაში, თუ ის აღნიშნული წარმოებისათვის დადგენილ წესებს არ აკმაყოფილებს. დაუშვებელია ადმინისტრაციული წარმოებისას და სასამართლოში სამართალწარმოებისას ელექტრონული ხელმოწერისათვის ან/და ელექტრონული შტამპისათვის მტკიცებულებითი ძალის მინიჭებაზე უარის თქმა მხოლოდ იმ მოტივით, რომ ის არ აკმაყოფილებს კვალიფიციური ელექტრონული ხელმოწერისათვის ან/და კვალიფიციური ელექტრონული შტამპისათვის ამ კანონით დადგენილ მოთხოვნებს.

მიუხედავად ზემოაღნიშნული დანაწესისა, თუ ფიზიკურ პირებს ან/და კერძო სამართლის იურიდიულ პირებს შორის შეთანხმება არსებობს, ელექტრონულ დოკუმენტსა და ელექტრონულ ხელმოწერას ამ პირებისათვის აქვს, შესაბამისად, მატერიალური დოკუმენტისა და პირადი ხელმოწერის თანაბარი იურიდიული ძალა. გარდა ამისა, საქართველოს ეროვნული ბანკისა და საფინანსო სექტორის წარმომადგენლების მიერ საქმიანობის განხორციელებისას ამ კანონისგან განსხვავებული პირობების შესაბამისად, საქართველოს ეროვნული ბანკის მიერ დადგენილი წესით შესრულებულ ელექტრონულ დოკუმენტსა და ელექტრონულ ხელმოწერას აქვს, შესაბამისად, მატერიალური დოკუმენტისა და პირადი ხელმოწერის თანაბარი იურიდიული ძალა[42].

კვალიფიციური ელექტრონული ხელმოწერისა და შტამპის სამართლებრივი პრობლემატიკის აღმოჩენისას განსაკუთრებული ყურადღება მათი ნამდვილობის დადგენას უნდა დაეთმოს. აღნიშნულს ითვალისწინებს „ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ“ საქართველოს კანონის მე-8 მუხლი. კვალიფიციური ელექტრონული ხელმოწერისა და კვალიფიციური ელექტრონული შტამპის ნამდვილობის კვალიფიციური დადგენა შემდეგი პირობების გათვალისწინებით ხორციელდება:

ა) კვალიფიციური ელექტრონული ხელმოწერის შესრულების/კვალიფიციური ელექტრონული შტამპის დასმის მომენტში აღნიშნული ხელმოწერა/შტამპი კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის სერტიფიკატს უნდა ეფუძნებოდეს;

[42] იხ. „ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ“ საქართველოს კანონის მე-3 მუხლი. https://matsne.gov.ge/ka/document/view/3654557?publication=0#DOCUMENT:1; (ბოლო ნახვის თარიღი 27.03.2021)

ბ) კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის სერტიფიკატი კვალიფიციური სანდო მომსახურების მიმწოდებლის მიერ უნდა იყოს გაცემული და კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის გამოყენების მომენტში მოქმედი უნდა იყოს;

გ) კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის შემოწმების მონაცემები უნდა შეესაბამებოდეს კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის ნამდვილობის კვალიფიციური დადგენის მომსახურების მიმღები მხარისთვის (მიმღები მხარე) წარდგენილ მონაცემებს;

დ) მონაცემთა ერთობლიობა, რომელიც უნიკალურად განსაზღვრავს ხელმომწერს/შტამპის დამსმელს და მოცემულია სერტიფიკატში, ზუსტად უნდა შეესაბამებოდეს მიმღები მხარისთვის წარდგენილ მონაცემებს;

ე) თუ კვალიფიციური ელექტრონული ხელმოწერა ფსევდონიმის გამოყენებით სრულდება, ამის თაობაზე უნდა ეცნობოს მიმღებ მხარეს;

ვ) კვალიფიციური ელექტრონული ხელმოწერა/კვალიფიციური ელექტრონული შტამპი კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის შესაქმნელი საშუალების გამოყენებით უნდა იყოს შექმნილი;

ზ) ხელმოწერილი მონაცემების მთლიანობა დაცული უნდა იყოს;

თ) კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის გამოყენებისას დაცული უნდა იყოს განვითარებული ელექტრონული ხელმოწერისათვის/განვითარებული ელექტრონული შტამპისათვის ამ კანონით დადგენილი მოთხოვნები.

უნდა აღინიშნოს, რომ კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის ნამდვილობის კვალიფიციური დადგენისათვის გამოყენებული სისტემა მიმღებ მხარეს უნდა აწვდიდეს ინფორმაციას ამ მუხლის პირველი პუნქტით განსაზღვრული პირობების დაკმაყოფილების შესახებ და უნდა იძლეოდეს მონაცემთა უსაფრთხოებასთან დაკავშირებული ნებისმიერი საკითხის გამოვლენის შესაძლებლობას. ამგვარი ხელმოწერისა და შტამპის ნამდვილობის კვალიფიციური დადგენას ახორციელებს კვალიფიციური სანდო მომსახურების მიმწოდებელი, რომელიც:

ა) კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის ნამდვილობას ამ მუხლის მოთხოვნათა შესაბამისად ადგენს;

ბ) მიმღებ მხარეს ავტომატურ რეჟიმში აწვდის კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის ნამდვილობის დადგენის შესახებ სანდო ინფორმაციას, რომელსაც აქვს კვალიფიციური სანდო მომსახურების მიმწოდებლის განვითარებული ელექტრონული ხელმოწერა/განვითარებული ელექტრონული შტამპი.

კანონის მე-9 მუხლი განსაზღვრავს კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის კვალიფიციური შენახვის საკითხს.

კვალიფიციური სანდო მომსახურების მიმწოდებელი უფლებამოსილია კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის კვალიფიციური შენახვის მომსახურების მიწოდებაზე, რაც გულისხმობს კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის სანდოობის გახანგრძლივებას მისი ტექნოლოგიური მოქმედების ვადის ამოწურვის შემდეგ.

როგორც აღინიშნა, ციფრული ხელმოწერა წარმოადგენს ელექტრონული ხელმოწერის ძირითად სახეს, რომელიც ტრადიციულ ელექტრონულ ხელმოწერასთან შედარებით მეტ დაცულობას უზრუნველყოფს.

ელექტრონული დოკუმენტის შედგენისას პრობლემური საკითხია მისი ავთენტიფიკაცია და ხელშეუხებლობა, რის გადაჭრაც ელექტრონული ციფრული ხელმოწერის მეშვეობით შეიძლება. ეს უკანასკნელი ყველაზე სანდო ხელმოწერაა და ეფუძნება სწორედ წყვილი – ღია და დახურული – გასაღების (ზოგჯერ მათ საჯარო და პირად გასაღებებსაც უწოდებენ) გამოყენებას. ელექტრონულ-ციფრული ხელმოწერა სიმბოლოთა ერთობლიობაა, რომლის გენერირებაც ხდება სპეციალური ალგორითმით – დოკუმენტის ტექსტისა და დოკუმენტის ხელმომწერი პირის პირადი კოდის „შერევით“[43]. როგორც ამ განმარტებიდანაც ჩანს, ელექტრონულ-ციფრული ხელმოწერა განუყოფლად აკავშირებს კონკრეტულ ელექტრონულ დოკუმენტს კონკრეტულ პირთან, უფრო ზუსტად კი, მისთვის ცნობილ ერთ კოდთან. თუ შევცვლით ელექტრონულ-ციფრული ხელმოწერით შესრულებულ დოკუმენტს, მის თუნდაც ერთ სიმბოლოს, ხელმოწერა აღარ დაემთხვევა.

ელექტრონულ-ციფრული ხელმოწერა ელექტრონული დოკუმენტის რეკვიზიტია, იგი გამიზნულია, გაყალბებისაგან დაიცვას მოცემული ელექტრონული დოკუმენტი, რომელიც ინფორმაციის კრიპტოგრაფიული გარდაქმნის შედეგადაა მიღებული ელექტრონულ-ციფრული ხელმოწერის დახურული გასაღების გამოყენებით და იძლევა გასაღების სერტიფიკატის მფლობელის იდენტიფიკაციის, ასევე ელექტრონულ დოკუმენტში ინფორმაციის შეცვლის (დამახინჯების) არარსებობის დადგენის საშუალებას. ამდენად, ელექტრონული ციფრული ხელმოწერა არის ელექტრონული ხელმოწერა, რომელიც ელექტრონული ჩანაწერის ტრანსფორმაციაა ასიმეტრიული კრიპტოსისტემის გამოყენებით. ამ პროცესის დროს პირს, რომელსაც აქვს საწყისი, არატრანსფორმირებული ელექტრონული ჩანაწერი და ხელმომწერი პირის საჯარო გასაღები, შეუძლია, ზუსტად განსაზღვროს: ა) მოხდა თუ არა ტრანსფორმაცია პირადი გასაღების გამოყენებით, რომელიც შეესაბამება ხელმომწერი პირის საჯარო გასაღებს; ბ) შეიცვალა თუ არა საწყისი ელექტრონული ჩანაწერი მას შემდეგ, რაც შესრულდა ტრანსფორმაცია[44].

---

[43] Bolam P./Choi R. Electronic signatures: when are they effective? Internet Law Bulletin LexisNexis October 2012 Vol 15 .No 7.p, 118

[44] ზამბახიძე თ. ელექტრონული ვაჭრობის სამართლებრივი რეგლამენტაციის საფუძვლები (პრობლემები და პერსპექტივა).ქართული სამართლის მიმოხილვა 8/2005-1/2.გვ, 124

ელექტრონულ დოკუმენტზე ციფრული ხელმოწერა მიიჩნევა მატერიალურ დოკუმენტზე პირადი ხელმოწერის თანაბარი იურიდიული ძალის მქონედ, თუ ფიცრული ხელმოწერა გამოიყენება ელექტრონული დოკუმენტის ხელმოწერის მომენტში მოქმედ სერტიფიკატში მითითებული მონაცემების შესაბამისად და შესაძლებელია ციფრული ხელმოწერის ნამდვილობის შემოწმება და დადასტურება[45].

სერტიფიკატის საფუძველზე შექმნილი ციფრული ხელმოწერით დამოწმებული ან/და დადასტურებული ელექტრონული დოკუმენტის გამოყენება შესაძლებელია ყველა შემთხვევაში, თუ საქართველოს კანონმდებლობა პირდაპირ არ მოითხოვს სერტიფიკატის საფუძველზე შექმნილი ციფრული ხელმოწერის გამოყენებას[46].

გარიგებების ელექტრონული გზით ხელმოწერისას აუცილებელია, რომ ხელმოწერა ასრულებდეს შემდეგ იურიდიულ ფუნქციებს: მიუთითებდეს, ვინ მოაწერა ხელი ელექტრონულ დოკუმენტს, იძლეოდეს გარანტიას, რომ ელექტრონული დოკუმენტი ხელმოწერილია უფლებამოსილი პირის მიერ, უზრუნველყოფდეს ხელმოწერილი დოკუმენტის ნამდვილობას, ნიშნავდეს გარიგების მხარეთა ნების გამოვლენას, ახდენდეს ელექტრონული გზით დადებული გარიგების წერილობითი ფორმის გარიგებად სიმბოლიზებას[47].

ელექტრონული შტამპი

„ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ“ საქართველოს კანონის [შემდეგომში, კანონის] მიხედვით, **ელექტრონული შტამპი** არის „ელექტრონულ მონაცემთა ერთობლიობა, რომელიც დაერთვის ან ლოგიკურად უკავშირდება ელექტრონულ დოკუმენტს და ელექტრონული დოკუმენტის მთლიანობისა და წარმომავლობის სისწორის დასადასტურებლად გამოიყენება“.

ელექტრონული ხელმოწერის მსგავსად, ელექტრონულ შტამპიც ითვალისწინებს განვითარებული ელექტრონული შტამპისა და კვალიფიციური ელექტრონული შტამპის ნაირსახეობებს.

განვითარებული ელექტრონული შტამპი წარმოადგენს ისეთ ელექტრონულ შტამპს, რომელიც აკმაყოფილებს შემდეგ მოთხოვნებს:

ა) იგი მხოლოდ შტამპის დამსმელთანაა დაკავშირებული;

ბ) მისი მეშვეობით შტამპის დამსმელის დადგენაა შესაძლებელი;

---

45 თუმანიშვილი გ. გარიგებები (სამართლებრივი ბუნება და ნორმატიული რეგულირება). თბ., 2012. გვ, 81-82

46 Wright C. Electronic Contracting In An Insecure World. SANS Institute 2008, p.7

47 ზამბახიძე თ. ელექტრონული ვაჭრობის სამართლებრივი რეგლამენტაციის საფუძვლები (პრობლემები და პერსპექტივა). ქართული სამართლის მიმოხილვა 8/2005-1/2..124

გ) იგი შექმნილია ელექტრონული შტამპის შექმნის იმ მონაცემების საშუალებით, რომელთა გამოყენებაც შტამპის დამსმელს, მტკიცე რწმუნებით, საკუთარი კონტროლით შეუძლია;

დ) იგი შტამპდასმულ მონაცემებთან ისეა დაკავშირებული, რომ მათი შემდგომი ცვლილების აღმოჩენის შესაძლებლობას იძლევა;

კვალიფიციური ელექტრონული შტამპი კი არის განვითარებული ელექტრონული შტამპის ნაირსახეობა, რომელიც კვალიფიციური ელექტრონული შტამპის შექმნის საშუალების გამოყენებით, კვალიფიციური ელექტრონული შტამპის სერტიფიკატის საფუძველზეა შესრულებული.

როგორც ზემოთაც აღინიშნა, ელექტრონული შტამპის სამართლებრივი რეგულაციები იდენტურია ელექტრონული ხელმოწერის მიმართ წაყენებული მოთხოვნებისა და შესაბამისად, კანონითაც მასთან ერთად რეგულირდება.

ელექტრონული ხელმოწერისა და შტამპის სერტიფიკატის გაუქმება

კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაუქმების შემთხვევაში მისი ხელახალი ამოქმედება დაუშვებელია.[48] კვალიფიციური ელექტრონული ხელმოწერა/კვალიფიციური ელექტრონული შტამპი, რომელიც კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაუქმების შემდეგაა შესრულებული/დასმული, ბათილია.

კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაუქმებისას, მოქმედების შეჩერებისას და ხელახალი ამოქმედებისას უნდა მიეთითოს შესაბამისი დრო და თარიღი, რომლებიც ეყრდნობა საერთაშორისო კოორდინირებულ დროსთან (UTC) დაკავშირებულ დროის ზუსტ წყაროს. დაუშვებელია ამ მოქმედებების წარსული დროისა და თარიღის მითითებით განხორციელება. კვალიფიციური სანდო მომსახურების მიმწოდებელმა კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაუქმება, მოქმედების შეჩერება და ხელახალი ამოქმედება შესაბამისი დროისა და თარიღის მითითებით, დაუყოვნებლივ უნდა აღრიცხოს.

კვალიფიციური სანდო მომსახურების მიმწოდებელი უფლებამოსილია, თავისი მომსახურების მომხმარებელს შესთავაზოს კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის სერტიფიკატის მოქმედების შეჩერების მომსახურება, რომელიც სერტიფიკატის მოქმედების დროებით შეჩერებას გულისხმობს. კვალიფიციური

[48] „ელექტრონული დოკუმენტისა და ელექტრონული სანდო მომსახურების შესახებ“ საქართველოს კანონი, მუხლი 10.

სანდო მომსახურების მიმწოდებელი ვალდებულია კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის სერტიფიკატის მოქმედების შეჩერების მომენტში გამოაქვეყნოს ინფორმაცია მისი შეჩერების შესახებ და უზრუნველყოს ამ ინფორმაციის ხელმისაწვდომობა აღნიშნული სერტიფიკატის მოქმედების შეჩერების მთელი პერიოდის განმავლობაში.

კანონი განსაზღვრავს კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის სერტიფიკატის მოქმედება-შეჩერების წინაპირობებს, რომლის მიხედვითაც, სერტიფიკატი ჩერდება: სერტიფიკატის მფლობელის მოთხოვნის საფუძველზე, საზედამხედველო ორგანოს დასაბუთებული მოთხოვნის საფუძველზე, კვალიფიციური სანდო მომსახურების მიმწოდებლის მიერ, შინაგანაწესით განსაზღვრულ შემთხვევაში და საქართველოს კანონმდებლობით გათვალისწინებულ სხვა შემთხვევებში.[49]

იმ კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის სერტიფიკატის ხელახალი ამოქმედების მოთხოვნა, რომლის მოქმედებაც შეჩერდა, შეუძლია აღნიშნული სერტიფიკატის მოქმედების შეჩერების ინიციატორს ან საქართველოს კანონმდებლობით გათვალისწინებულ უფლებამოსილ პირს.

კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის სერტიფიკატი უქმდება: ა) სერტიფიკატის მფლობელის მოთხოვნის საფუძველზე; ბ) სერტიფიკატის მოქმედების შეჩერებიდან 10 კალენდარული დღის გასვლის შემდეგ, თუ ამ პერიოდში აღნიშნული სერტიფიკატი ხელახლა არ ამოქმედდა; გ) კვალიფიციური სანდო მომსახურების მიმწოდებლის მიერ, შინაგანაწესით განსაზღვრულ შემთხვევაში; დ) კვალიფიციური სანდო მომსახურების მიმწოდებლის მიერ მომსახურების მიწოდების შეწყვეტის შემთხვევაში, თუ კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაცემისა და მომსახურების მიწოდების უფლებამოსილება სხვა პირს არ გადაეცა და ე) საქართველოს კანონმდებლობით გათვალისწინებულ სხვა შემთხვევებში.[50]

კვალიფიციური სანდო მომსახურების მიმწოდებელმა კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის სერტიფიკატის მფლობელს დაუყოვნებლივ უნდა აცნობოს კვალიფიციური ელექტრონული ხელმოწერის/კვალიფიციური ელექტრონული შტამპის სერტიფიკატის გაუქმების, მოქმედების შეჩერებისა და ხელახალი ამოქმედების შესახებ.

კვალიფიციური სანდო მომსახურების მიმწოდებლის ავტორიზაციისა და ზედამხედველობის ფუნქციას 2020 წლის 20 ივნისამდე ასრულებდა საქართველოს იუსტიციის სამინისტროს მმართველობის სფეროში მოქმედი სსიპ – მონაცემთა გაცვლის სააგენტო. 2020 წლის

[49] იქვე, მე-10 მუხლის მე-4 მუნქტი.
[50] იქვე, მე-10 მუხლის მე-6 პუნქტი.

20 ივნისს მიღებული იქნა კანონი „საჯარო სამართლის იურიდიული პირის – ციფრული მმართველობის სააგენტოს შესახებ“, რომელმაც გააერთიანა სამინისტროს შემადგენლობაში შემავალი ორი ს.სიპ – მონაცემთა გაცვლის სააგენტო და „სმართ ლოჯიქი“ (SMART LOGIC). შესაბამისად, ამ პერიოდიდან კვალიფიციური სანდო მომსახურების ზედამხედველობის ფუნქციას ციფრული მმართველობის სააგენტო ასრულებს.

უნდა აღინიშნოს, რომ ევროკავშირის ქვეყნებში ელექტრონული ხელმოწერის საკითხების ერთგვაროვან რეგლამენტაციას უზრუნველყოფს დირექტივა „ელექტრონული ხელმოწერის შესახებ“, ხოლო UNSITRAL-ის ელექტრონული ვაჭრობის სამუშაო ჯგუფის 31-ე-38-ე სესიები მიეძღვნა მოდელური კანონის შექმნას „ელექტრონული ხელმოწერების შესახებ“. 1999 წლის დირექტივამ დაადგინა ელექტრონული ხელმოწერისა და ელექტრონული ხელმოწერის გასაღების სერტიფიკატის გაცემაზე მომსახურების გაწევის „ჩარჩო“ რეგულირება, რათა ევროკავშირის მონაწილე სახელმწიფოებს ამ დირექტივის შესაბამისად მიეღოთ კანონები და კანონქვემდებარე აქტები[51].

კანონმდებლობამ უნდა უზრუნველყოს, რომ ელექტრონული ხელმოწერები, რომლებიც შექმნილია ელექტრონული ციფრული ხელმოწერის საიმედო საშუალებების გამოყენებით და აქვს შესაბამისი სერტიფიკატი: ა) აკმაყოფილებდეს ელექტრონული ფორმის მონაცემთა მიმართ ხელმოწერის იურიდიულ მოთხოვნებს ისევე, როგორც პირადად სუბიექტის მიერ ქაღალდზე ასახულ ინფორმაციაზე განხორციელებული ხელმოწერა; ბ) ელექტრონული საშუალებით ხელმოწერილი დოკუმენტი დაიშვებოდეს, როგორც სასამართლო მტკიცებულება. აუცილებლად უნდა აღვნიშნოთ ელექტრონული ხელმოწერების მარეგულირებელი კანონმდებლობისადმი ისეთი საყოველთაოდ აღიარებული მიდგომა, როგორიცაა ე.წ. „ტექნოლოგიური ნეიტრალურობა“. პირადი ხელმოწერის ნებისმიერი ელექტრონული ანალოგის სამართლებრივი აღიარება და მათი იურიდიული ძალა არ იზღუდება გამოყენებული ტექნოლოგიის მიხედვით. ელექტრონული ხელმოწერა მხოლოდ გამოყენებული სამართლის მოთხოვნებს უნდა პასუხობდეს. სწორედ ამ მიზეზით ელექტრონული ვაჭრობის საკითხებზე მომუშავე UNCITRAL-ის სამუშაო ჯგუფმა უარი თქვა „კრიპტოგრაფიული გასაღების“ ცნების შემოტანაზე „ელექტრონული ხელმოწერების შესახებ“ მოდელური კანონის პროექტში, რადგან იგი არ პასუხობდა ნეიტრალურობის პრინციპს, რომელიც პროექტის საფუძველი იყო[52].

[51] ზამბახიძე თ. ელექტრონული ვაჭრობის სამართლებრივი რეგლამენტაციის საფუძვლები (პრობლემები და პერსპექტივა). ქართული სამართლის მიმოხილვა 8/2005-1/2.გვ, 124

[52] იქვე, გვ. 127

კიბერუსაფრთხოება

ძირითადი გამოწვევები

ევროკავშირის ქსელისა და ინფორმაციის უსაფრთხოების სააგენტოს (ENISA)[53] შეფასებით „კიბერჰიგიენა პირადი ჰიგიენის მსგავსად უნდა განვიხილოთ და ორგანიზაციაში სწორად დანერგვის შემდეგ ის იქცევა ყოველდღიური რუტინის ნაწილად, სწორ ჩვევებად და პერიოდულ შემოწმებად, რათა დავრწმუნდეთ, რომ ორგანიზაციის „ონლაინ ჯანმრთელობა“ ოპტიმალურ მდგომარეობაშია“.

მრავალი ორგანიზაცია მხოლოდ კიბერუსაფრთხოების პროფესიონალებს ეყრდნობა, რათა ყოველდღიური სამუშაო პროცესის დროს დაიცვას საკუთარი და მისი საბოლოო მომხმარებლის მონაცემები.

ამ დროს ყველაზე მნიშვნელოვანი საკითხია ნებისმიერი თანამშრომლის ცნობიერების ამაღლება კიბერჰიგიენის საკითხებში, რადგან ორგანიზაციის კომპიუტერულ ქსელში წარმატებული შეღწევის უდიდესი ნაწილის მიზეზი თანამშრომლის არასწორი ქმედებაა. არასწორი არ ნიშნავს გამიზნულ ქმედებას, არამედ უფრო კიბერჰიგიენის საკითხების არცოდნასთან გვაქვს საქმე. ამიტომ თითოეულ თანამშრომელს უნდა ესმოდეს, რა არის კიბერჰიგიენა და მათი როლი ორგანიზაციის ინფორმაციის დაცვაში.

მავნე კოდი, ვირუსები, ჯაშუში პროგრამები

მავნე კოდის შემცველი აპლიკაციების მიზანია თქვენი ფაილების დაზიანება, პერსონალური, კონფიდენციალური ან სხვა ტიპის ინფორმაციის მოპარვა. შესაძლებელია, მავნე აპლიკაციამ თქვენი მოწყობილობა სხვებზე შეტევისთვის გამოიყენოს. მავნე აპლიკაციები კიბერკრიმინალებს საშუალებას აძლევენ: მიწვდნენ პირად და ბიზნეს კონტაქტებს, გააგზავნონ „ფიშინგ“ წერილები ან ტექსტური შეტყობინებები, გამოიყენონ ხელსაწყო კომპიუტერულ ქსელთან დასაკავშირებლად, განახორციელონ ზარები, განახორციელონ შესყიდვები საკრედიტო ბარათით, გადარიცხონ თანხები საბანკო ანგარიშებიდან, დაიწყონ მიყურადება ან ჩაწერონ ხმა ან ვიდეო თქვენი ხელსაწყოს გამოყენებით და გადაიტანონ ეს ინფორმაცია რომელიმე cloud service-ზე.

მავნე აპლიკაციების გავრცელების ერთ-ერთი მეთოდია უფასო უკაბელო ქსელები (WiFi). მათთან დაკავშირებისას მარტივად შეიძლება თქვენს მოწყობილობაში მავნე კოდის შემცველმა აპლიკაციამ შემოაღწიოს. ზოგადად, მავნე ფაილების გავრცელებისა და შეტევისთვის მობილური მოწყობილობები უფრო საინტერესო სამიზნეა, ვიდრე თავად კომპიუტერები. კიბერკრიმინალების ერთ-ერთი ტაქტიკაა მავნე აპლიკაციების გამოყენება, რაც აინფიცირებს მოწყობილობას და ხელმისაწვდომს ხდის პირად და ბიზნესინფორმაციას, შესაძლებელს ხდის მოწყობილობის კონტროლსაც.

[53] ENISA – https://www.enisa.europa.eu/

კიბერკრიმინალებს შეუძლიათ აგრეთვე გამოიყენონ ლეგიტიმური აპლიკაციების სუსტი მხარეები, ჩააშენონ მასში მავნე კოდები ისე, რომ აპლიკაციის შემქმნელებმა ამაზე არაფერი იცოდნენ.

ვირუსები და მავნე ფაილები ხშირად თქვენს კომპიუტერში მომაბეზრებელი, თუმცა თვალშისაცემი და მიმზიდველი რეკლამების გზით ხვდებიან. თუ შეთავაზება მეტისმეტად კარგად ჟღერს საიმისოდ, რომ სიმართლე იყოს, ალბათ არც არის მართალი. ამიტომ უნდა გვახსოვდეს, რომ ასეთი რეკლამის გახსნა დიდ რისკს უკავშირდება და ასე ჩვენ თვითონვე შემოვუშვებთ მავნე კოდის შემცველ აპლიკაციას ჩვენსავე მოწყობილობაში.

პაროლების პოლიტიკა

რა არის პაროლი? როგორც ვიცით, რაიმე სისტემაში ავთენტიფიკაციისას ჩვენ ვიყენებთ მომხმარებლის სახელს, რომელთანაც ერთადაც აუცილებელია პაროლის ცოდნაც, რათა სისტემამ ლეგიტიმურ მომხმარებლად აღგვიქვას. ზოგ შემთხვევაში, მაგალითად, საბანკო ბარათისა და ელექტრონული პირადობის მოწმობის შემთხვევაში, PIN კოდი, რომელიც მათი გამოყენებისას გვჭირდება, ასევე პაროლის ნაირსახეობაა. პირველი წესი, რაც პაროლთან დაკავშირებით უნდა ვიცოდეთ, ისაა, რომ არასდროს, არცერთ შემთხვევაში, **ჩვენი პაროლი სხვას არ უნდა გავუზიაროთ** და თუ ჩვენი პაროლი ვინმესთვის რაიმე გზით გახდა ცნობილი, დაუყოვნებლივ უნდა შევცვალოთ იგი.

ასევე უნდა იზრუნოთ იმაზე, რომ თქვენი პაროლი ადვილად გამოსაცნობი არ იყოს. პაროლის გამჟღავნების შემთხვევაში შესაძლოა დავკარგოთ ფული, პერსონალური მონაცემები, შესაძლოა სხვა პიროვნებამ ჩვენი სახელით ჩაიდინოს დანაშაული და ა.შ.

სხვისი პაროლის დაუფლების უმეტესი შემთხვევები გამოწვეულია იმით, რომ მომხმარებელს სუსტი ან სისტემის მიერ რეგისტრაციისას შეთავაზებული (default) პაროლი აქვს გამოყენებული, რომელსაც პერიოდულად არ ცვლის. მნიშვნელოვანია, რომ სხვადასხვა ელფოსტის შემთხვევაში სხვადასხვა პაროლი გამოვიყენოთ, რათა მესამე პირმა ერთი ელფოსტის კომპრომეტირების შემთხვევაში წვდომა არ მიიღოს ჩვენს ყველა ელფოსტაზე, **მათ შორის კორპორაციულზეც**.

პაროლის მოფიქრებისას უნდა გავითვალისწინოთ შემდეგი:

- უნდა შევარჩიოთ რაიმე ფრაზა სიმღერიდან, ფილმიდან, წიგნიდან ან ნებისმიერი ტექსტიდან, რომელიც გვახსოვს;
- შეიძლება გამოვიყენოთ ფრაზის შემადგენელი სიტყვების პირველი ასოები;
- პაროლი უნდა შეიცავდეს დიდ ასოს, პატარა ასოს, სიმბოლოს და ციფრს ერთდროულად;
- პაროლი უნდა იყოს 8-დან 12-მდე სიმბოლოსგან შემდგარი;
- პაროლი უნდა იყოს რთული, რომ შეუძლებელი იყოს მისი ლოგიკურად გამოცნობა.

ელექტრონული ფოსტა

დღევანდელი საქმიანობა წარმოუდგენელია ელექტრონული ფოსტის გარეშე. მისი საშუალებით მარტივია წერილის მიწერა, ინფორმაციის გაზიარება, ზოგადად, კომუნიკაცია, მაგრამ ამ საშუალებას თან ახლავს გარკვეული რისკები, მაგალითად, არაავტორიზებული წვდომა მონაცემებზე, მონაცემების შეცვლა, DOS (Denial of Service – შეტევა ერთი მისამართიდან) შეტევის ტიპი, რომელიც გულისხმობს სერვისის მწყობრიდან გამოყვანას; DDOS (Distributed denial of Service – შეტევა რამდენიმე მისამართიდან) შეტევები, მონაცემებისა და ფაილების უსაფრთხოება.

ელექტრონულ ფოსტასთან დაკავშირებული რისკებია:

სპამი

არასასურველი ელექტრონული შეტყობინებები. სპამი ეგზავნება ძალიან ბევრ მომხმარებელს. სპამის დასაგზავნად ელფოსტის ლეგიტიმურ მისამართებს ყიდულობენ შავ ბაზარზე ან იღებენ სოციალური ქსელებიდან, ფორუმებიდან. ამიტომ მნიშვნელოვანია ვიცოდეთ, სად და რა მიზნით შეგვყავს ხოლმე ჩვენი ელფოსტის მისამართი.

ფიშინგი

როგორც წესი, ფიშინგ ელფოსტას უცხო ქვეყნებიდან აგზავნიან. ამიტომ, ასეთი ელექტრონული წერილის მიღებისას ტექსტში ხშირად არის გრამატიკული ან მართლწერის შეცდომები. ასეთი წერილები წაკითხვისას გადაუდებლობის განცდას აჩენს – უმეტესად შემოთავაზება მეტისმეტად კარგი და დაუჯერებელია. ზოგიერთ შემთხვევაში კი გამომგზავნი დაშინების მცდელობას მიმართავს.

თუ სასწრაფო ელფოსტა მიიღეთ, გადაამოწმეთ, სანამ მიღებულ ინსტრუქციებს შეასრულებდეთ. არ დაიზაროთ დარეკვა იმ ადამიანთან (იმ ნომერზე არა, რომელიც მეილშია მითითებული), ვისი სახელითაც გთხოვენ მოქმედებას.

შეამოწმეთ გამომგზავნის მისამართი – ორჯერ დააწკაპუნეთ გამომგზავნის სახელს და ნახავთ, რეალურად რომელი მისამართიდან მოგივიდათ წერილი.

არ გადაუგზავნოთ საეჭვო წერილი სხვა კოლეგებს, თქვენ შეიძლება მიხვდეთ, რომ ფიშინგ წერილია, ხოლო სხვა – ვერა.

მავნე კოდის შემცველი ფაილების მიმაგრება

ელფოსტას ხშირად თან ახლავს ხოლმე მიმაგრებული ფაილი. ხშირად ადამიანი ბოლომდე არ კითხულობს წერილს და პირდაპირ ხსნის მიმაგრებულ ფაილს. ამ დროს კი ეს ფაილი შეიძლება შეიცავდეს ვირუსს, რომელიც გახსნისას დააზიანებს თქვენს ფაილებს და შემდეგ თქვენი ორგანიზაციის ქსელში გავრცელდება.

ამიტომ გასათვალისწინებელი შემდეგი:

- არასოდეს გახსნათ უცნობი პირისაგან ელფოსტით გამოგზავნილი ფაილები;
- ასევე არ გახსნათ ნაცნობი პირისაგან ელფოსტით გამოგზავნილი უცნაური/საეჭვო ფაილები;
- ეჭვის გაჩენის შემთხვევაში აუცილებლად დაუკავშირდით ტექნიკურ ჯგუფს.

საფრთხის შემცველი ბმულების მიმაგრება ფოსტის ტექსტში

ხშირად მოდის წერილები, რომლებშიც ინტერნეტბმულებია (Link) მითითებული. ბმულზე დაჭერით ბრაუზერში შესაძლოა ისეთი მისამართი გახსნათ, რომლიდანაც თქვენს კომპიუტერში ავტომატურად გაეშვება მავნე ფაილი.

იმისათვის, რომ გაარკვიოთ, ბმულზე დაჭერით იმ მისამართს გახსნით თუ არა, რომელსაც ბმულის შეხედვისას ფიქრობთ, მაუსი, მასზე დაჭერის გარეშე, უნდა მიიტანოთ ბმულთან და ეკრანზე გამოჩნდება, რეალურად რომელ მისამართზე გადახვალთ მასზე დაჭერის შემთხვევაში.

კონფიდენციალური მონაცემების ღიად გაზიარება

ელფოსტით კომუნიკაცია ღია კომუნიკაციაა და, შესაბამისად, ნაკლებად უსაფრთხოა კონფიდენციალური ინფორმაციის გასაგზავნად. თუ მნიშვნელოვანი ინფორმაცია გაქვთ გასაგზავნი, შესაძლებელია ფაილების დაარქივება და მისი პაროლით დაცვა. ამის შემდეგ შეგიძლიათ პაროლით დაცული არქივის ფაილი ადრესატთან გააგზავნოთ.

მობილური მოწყობილობები

ჩვენი უმეტესობა სამსახურებრივი მოვალეობის შესრულებისას საკუთარ სმარტფონებს (Smart phone) ვიყენებთ.

შესაბამისად, აუცილებელია დავფიქრდეთ:

- რა სახის მონაცემებს ვამუშავებთ და ვინახავთ სმარტფონში;
- რა სახის ავთენტიფიკაციის მეთოდებს ვიყენებთ სმარტფონით მუშაობისას;
- ვართ თუ არა დაცულები მავნე ფაილებისაგან;
- ვიყენებთ თუ არა დაშიფრული კომუნიკაციის მეთოდს;
- უყურადღებოდ ხომ არ ვტოვებთ ხოლმე ჩვენს სმარტფონს;
- ხშირად გვაქვს თუ არა ჩართული Bluetooth;
- ჩართული გვაქვს თუ არა მონაცემების სინქრონიზაცია.

მნიშვნელოვანია, სმარტფონში კონფიდენციალური ან საიდუმლო ინფორმაციის შენახვა-დამუშავებას თავი ავარიდოთ. აუცილებელია, ეკრანის გასააქტიურებლად დაყენებული გვქონდეს PIN ან სხვა სახით ავთენტიფიკაციის მოთხოვნა. რეკომენდებულია, სმარტფონში შენახული მონაცემები დაშიფრული იყოს, რაშიც ტექნიკური სამსახური უნდა დაგეხმაროთ. აუცილებელია ანტივირუსის გამოყენება. მნიშვნელოვანია, რომ სმარტფონი ყოველთვის თან გვქონდეს და უყურადღებოდ არ დავტოვოთ, რადგან ამ დროს შეიძლება სხვა პირმა სცადოს მასზე წვდომა. რეკომენდებულია, სმარტფონს ჰქონდეს მონაცემების დისტანციურად წაშლის შესაძლებლობა (WIPE feature), რათა დაკარგვის შემთხვევაში წავშალოთ ისინი.

უკაბელო ქსელები

აუცილებელია გახსოვდეთ, რომ ყველა ღია უკაბელო ქსელი (WiFi) საფრთხის შემცველად ითვლება და მათი გამოყენება რეკომენდებული არ არის. თუ ღია ქსელით მაინც სარგებლობთ, ამ დროს არ შეხვიდეთ არცერთ კორპორაციულ სისტემაში, რათა ამ დროს მასზე წვდომა არ მიიღოს მესამე პირმა.

სოციალური ინჟინერია

სოციალური ინჟინერია არის პროცესი, როდესაც ერთი პირი მეორეს აიძულებს იმის გაკეთებას, რასაც ჩვეულებრივ შემთხვევაში უცხოსთვის არ გააკეთებდა.

სოციალური ინჟინერიის ტიპებია:

Phone Phreaking: ჰაკერული შეტევა, როდესაც შემტევს ეძლევა შესაძლებლობა, შევიდეს სატელეფონო ქსელში და დაეუფლოს სატელეფონო კომპანიის ხელთ არსებულ ნებისმიერ ინფორმაციას.

Crackers or Vandals: ჰაკერები, რომლებიც ანადგურებენ ადამიანების ფაილებს და ხანდახან მყარ დისკებსაც.

Grifter: ადამიანი, რომელიც ტყუილით და დარწმუნებით მოიპოვებს ინფორმაციას კომპანიების შესახებ.

შეტევა შესაძლოა განხორციელდეს სხვადასხვა საშუალებით და ნებისმიერ ადგილას. მაგალითად, მობილურის ან კომპიუტერის გამოყენებით, სახლში ან სამსახურში. თქვენ გგონიათ, რომ რომელიმე ორგანიზაციის ლეგიტიმურ წარმომადგენელთან ან თქვენთვის კარგად ნაცნობ ადამიანთან გაქვთ კომუნიკაცია და სინამდვილეში თაღლითი მოტყუებით ცდილობს თქვენგან მისთვის საჭირო ინფორმაციის მიღებას. მას შემდეგ, რაც თაღლით

თქვენს მოწყობილობაზე წვდომას დაეუფლება, საფრთხე შეგექმნებათ როგორც სახლის სხვა მოწყობილობებზე, ასევე სამსახურის სისტემებზეც.

ფიშინგი – თაღლითობა

ფიშინგი შეტევის ერთ-ერთი გავრცელებული ტიპია. ამ დროს ხშირად ელფოსტაზე იღებთ თითქოს თქვენთვის საინტერესო ინფორმაციას, სადაც გთავაზობენ, გადახვიდეთ ელფოსტის ტექსტში მითითებულ ვებგვერდზე ან ბმულზე. შესაძლოა, ელფოსტით მიიღოთ შეტყობინება, რომ თქვენი ინტერნეტბანკის მომხმარებლის პაროლს ვადა გასდის, რის გამოც მითითებულ ბმულზე გადასვლას და პაროლის შეცვლას გთხოვენ.

იმისათვის, რომ ფიშინგის მსგავს შეტევებს მაქსიმალურად თავი ავარიდოთ, აუცილებელია:

- ეჭვი შევიტანოთ უცხო და არასაიმედო მეილებში;
- არ დავაჭიროთ ბმულებს, სანამ არ გადავამოწმებთ, კონკრეტულად რა მისამართზე გადავყავართ მას;
- ყოველი საეჭვო შემთხვევის შესახებ უნდა ვაცნობოთ ორგანიზაციის ტექნიკურ გუნდს;
- არასოდეს გავამჟღავნოთ ჩვენი პაროლები;
- ყველა ფაილი ანტივირუსს შევამოწმებინოთ;
- მოვერიდოთ ფაილების ჩამოტვირთვას არასანდო წყაროებიდან.

კიდევ ერთხელ, უნდა გვახსოვდეს, რომ სოციალური ინჟინერი უფლებამოსილი პირის მიერ მოთხოვნის წაყენების იმიტაციას ახდენს. როდესაც უცხო პირი რაიმეს შესრულებას გთხოვთ, უნდა გადაამოწმოთ ეს ინფორმაცია თავად ან ტექნიკურ სამსახურთან ერთად და დარწმუნდეთ, რომ მოთხოვნა ლეგიტიმურია.

რამდენიმე რჩევა:

- ელფოსტის პაროლის მოთხოვნა არცერთ შემთხვევაში არ არის დასაშვები;
- ჩამოტვირთვისას ყოველი ფაილი აუცილებლად დაასკანირეთ ანტივირუსის მეშვეობით;
- გადაამოწმეთ წყაროს სანდოობა, საიდანაც აპირებთ ინფორმაციის ჩამოტვირთვას;
- თუ თქვენი ძალებით ვერ გაერკვიეთ სიტუაციაში, დაუკავშირდით ტექნიკურ სამსახურს.

ელექტრონული მმართველობის ხელშემწყობი საინტერესო გადაწყვეტები

ხელოვნური ინტელექტის გამოყენების პრაქტიკული ასპექტები

ელექტრონული მმართველობის თანამედროვე მოდელებში დიდი როლი ენიჭება ახალი ტექნოლოგიების გამოყენებას. ამის ნათელი მაგალითია ხელოვნური ინტელექტის გამოყენება ცალკეული საჯარო მმართველობის საკითხების გადაწყვეტაში.

ხელოვნური ინტელექტის დეფინიცია საკმაოდ რთული შინაარსისაა. საქართველოს კანონმდებლობაც არ განსაზღვრავს ხელოვნური ინტელექტის ცნებას[54]. ამავდროულად, ხელოვნურ ინტელექტსა და სხვა ტიპის ფუნქციურ ალგორითმებს[55] შორის ყოველთვის ზღვარი თვალსაჩინო არ არის. თუმცა სირთულე არა მხოლოდ მის განმარტებაშია, არამედ მის დინამიკურ განვითარებაშიც. ხელოვნური ინტელექტი იმდენად სწრაფად ვითარდება, რომ წარმოუდგენელია მისი თუნდაც ათი ან ოცი წლის წინანდელი დეფინიციის უდავოდ აღიარება დღევანდელ რეალობაში. დღეს ხელოვნური ინტელექტის შესაძლებლობები და გამოყენების არეალი ისე გაიზარდა, რომ პრაქტიკულად ყველა სფერო მოიცვა.

ცნება „ხელოვნური ინტელექტის“ ავტორი პროფ. ჯონ მაკარტი ჯერ კიდევ 1956 წელს აღნიშნავდა, „პრობლემა ისაა, რომ ჩვენ ჯერ არ შეგვიძლია განვსაზღვროთ, რომელ გამოთვლით პროცედურებს შეიძლება ვუწოდოთ ინტელექტუალური. ჩვენ გვესმის ინტელექტის ზოგიერთი მექანიზმი, მაგრამ არ გვესმის სხვა დანარჩენი. ამიტომ ინფორმატიკის მეცნიერების თვალსაზრისით, ინტელექტის ცნების ქვეშ უნდა ვიგულისხმოთ მხოლოდ მსოფლიო მიზნების მისაღწევად გამოსაყენებელი გამოთვლითი შესაძლებლობები“[56].

მაგრამ ეს დეფინიცია მხოლოდ მეოცე საუკუნის ორმოცდაათიანი წლებისთვის შეიძლება იყოს მისაღები. დღეს ხელოვნური ინტელექტის მასშტაბები წარმოუდგენლადაა გაზრდილი და მეცნიერებაში ხელოვნური ინტელექტის განვითარების (გენერაციის) სამ საფეხურზე საუბრობენ. სწორედ განვითარების საფეხურების მიხედვით ხელოვნური ინტელექტი შეიძლება სამ ტიპად დავყოთ: ვიწრო ხელოვნური ინტელექტი; ზოგადი ხელოვნური ინტელექტი; სუპერ ხელოვნური ინტელექტი.

---

54 ხელოვნური ინტელექტის სისტემის გამოყენება საქართველოში. კანონმდებლობა და პრაქტიკა, IDFI-ს კვლევა, თბ. 2021, გვ. 8 იხ. https://idfi.ge/public/upload/Article/AI%20ENG%20FULL.pdf (ბოლო ნახვის თარიღი 27.03.2021)

55 ალგორითმი არის პროგრამული ინსტრუქციების კრებული, რომელიც მონაცემების დამუშავების შედეგად ავტომატურ რეჟიმში იღებს გადაწყვეტილებებს. ხელოვნური ინტელექტი კი უფრო ფართო ცნებაა და ალგორითმების ნაკრებს გულისხმობს. ამგვარი სისტემები, პროგრამის მიერ დამუშავებული მონაცემების საფუძველზე, ადამიანის ჩარევის გარეშე, თავად ქმნიან საკუთარ ალგორითმებს შეყვანილი მონაცემებისა და მონაცემების დამუშავების შედეგად გამოვლენილი ახალი გარემოებების მიხედვით (მანქანური სწავლება).

56 John McCarthy. What is Artificial Intelligence? http://www-formal.stanford.edu/jmc/whatisai/whatisai.html

ვიწრო ხელოვნური ინტელექტი (Narrow Artificial Intelligence – NAI)

ვიწრო ხელოვნური ინტელექტი ხელოვნური ინტელექტის განვითარების პირველი გენერაციაა. ეს ეტაპი თანამედროვე მეცნიერებას უკვე მიღწეული აქვს. ვიწრო ხელოვნური ინტელექტის მიზანია ერთ კონკრეტულ მიმართულებაში შეძლოს განვითარება და სრულყოფა. ამის მაგალითია დღეს არსებული, ათობით სფეროში ჩართული ხელოვნური ინტელექტის პროგრამები. ვიწრო ხელოვნური ინტელექტის დიდ წარმატებად მიიჩნევა ცნობილი ფაქტი, როდესაც კომპიუტერმა ჭადრაკი მოუგო მსოფლიო ჩემპიონ გარი კასპაროვს[55]. დღეს ვიწრო ხელოვნური ინტელექტის პროგრამები წარმატებით საქმიანობენ მედიცინასა და ჯანდაცვაში, ტრანსპორტში და ლოგისტიკაში, განათლებასა და მეცნიერებაში, აგრარულ სექტორსა და ეკონომიკაში, თვით მართლმსაჯულებაშიც კი[56].

ზოგადი ხელოვნური ინტელექტი (General Artificial Intelligence – GAI)

ზოგადი ხელოვნური ინტელექტი წარმოადგენს განვითარების შემდგომ ეტაპს (ახალ გენერაციას), რომლის დროსაც კომპიუტერულმა პროგრამამ უნდა შეძლოს საკუთარ შეცდომებზე სწავლა და თვითგანვითარების ისეთი ეტაპის მიღწევა, როცა ის ადამიანისგან დამოუკიდებლად შეძლებს ანალიტიკური აზროვნების განვითარებასა და დამოუკიდებლად დასახული ამოცანების გადაწყობას.

დღეისათვის ეს თანამედროვე მეცნიერების ერთ-ერთი ყველაზე დიდი გამოწვევაა. მეცნიერები არ კარგავენ იმედს, რომ შეძლებენ იმგვარი ალგორითმების შექმნას, რომელსაც თვითგანვითარება შეეძლება. ამგვარ იმედს ამყარებს თანამედროვე მეცნიერების ერთ-ერთი ყველაზე დიდი გამოგონების – ხელოვნური ნეირონული ქსელების გაჩენა. ხელოვნური ნეირონული ქსელი ხელოვნური ნეირონებისა და ამ ნეირონების დამაკავშირებელი წახნაგებისაგან შემდგარი ქსელია.

---

[57] ცნობილია, რომ გარი კასპაროვი ისტორიაში ერთ-ერთი ყველაზე ძლიერი მოთამაშეა. ის მეცამეტე მსოფლიო ჩემპიონია ჭადრაკში და ამ ტიტულის შენარჩუნება კასპაროვმა 1985 წლიდან 1993 წლამდე შეძლო. უკვე ოც წელზე მეტი გავიდა, მას შემდეგ, რაც ცნობილმა კომპიუტერმა Deep Blue-მ გარი კასპაროვი დაამარცხა. ამის შესახებ მთელი მსოფლიოს მაშინდელი პრესა წერდა. მიუხედავად ამისა, გარი კასპაროვი დღემდე ხელოვნური ინტელექტის პოპულარიზაციის აქტიური მომხრეა. ერთ-ერთ ინტერვიუში მან განაცხადა, რომ „კაცობრიობამ არ უნდა გაუწიოს წინააღმდეგობა ცვლილებებს, რომლებიც ხელოვნური ინტელექტის მქონე მანქანებს მსოფლიოსთვის მოაქვთ“. როცა მას შეახსენეს თანამედროვე მეცნიერების ერთ-ერთი უდიდესი წამომადგენლის, სტივენ ჰოკინგის სიტყვები „ხელოვნური ინტელექტის განვითარებას შესაძლოა მოჰყვეს როგორც პოზიტიური ასევე კაცობრიობისთვის დამღუპველი შედეგი. უნდა გავიაზროთ საფრთხე, რაც ამას მოჰყვება“, გარი კასპაროვმა უპასუხა: „ჩვენ ყველას გვაქვს იმის შიში, რომ ოდესღაც მოვკვდებით და რობოტები ჩაგვანაცვლებენ. მე მჯერა, რომ ადამიანის ფანტაზია ულევია და მას ვერასდროს დაეწევა მანქანის გონება. ჩვენი საქმეა მუდმივი ოცნება და სამყაროსთვის სასარგებლო ნივთების მოგონება, რომელიც მომავალ თაობას ცხოვრებას გაუმარტივებს“.

[58] აშშ-ში ფუქციონირებს ხელოვნური ინტელექტი, რომელიც ალგორითმის საფუძველზე განიხილავს განქორწინებასთან და მის შედეგად ქონების გაყოფასთან დაკავშირებულ საქმეებს. ესტონეთის მთავრობის დავალებით ქვეყნის იუსტიციის სამინისტრო აქტიურად მუშაობს ხელოვნური ინტელექტის შექმნაზე, რომლის მიზანსაც წვრილმან სამოქალაქო საქმეებზე გადაწყვეტილებების მიღება წარმოადგენს. ესტონეთის მთავრობა იმედოვნებს, რომ ამ რეფორმით მოახერხებს სასამართლოების გადატვირთულობის პრობლემის გადაჭრას.

ზოგიერთი წახნაგი მოცემული ნეირონისთვის განიხილება შემომავლად, ხოლო ზოგიერთი – გამავლად. ყოველი წახნაგი ხასიათდება წონით, რომელიც ზოგ მოდელებში შეიძლება დროთა განმავლობაში შეიცვალოს. ხელოვნური ნეირონული ქსელის მოდელი ადამიანის ბუნებრივი ნეირონული ქსელის მიხედვითაა აღებული, რამაც თანამედროვე კომპიუტერებს წარმოუდგენლად დიდი შესაძლებლობები მისცა და დაუშვა ალბათობა იმისა, რომ მომავალში ადამიანებმა შეიძლება სუპერ ხელოვნური ინტელექტიც შექმნან.

სუპერ ხელოვნური ინტელექტი (Super Artificial Intelligence – SAI)

დღეისათვის სუპერ ხელოვნური ინტელექტი მხოლოდ თეორიაა და უფრო ფანტასტიკური ფილმებიდანაა ცნობილი. მას არავითარი რეალური მეცნიერული საფუძველი არ გააჩნია. სუპერ ხელოვნური ინტელექტის იდეაა, რომ ზოგადი ხელოვნური ინტელექტის შექმნის შემთხვევაში შეიძლება ამ უკანასკნელმა თვითგანვითარების ისეთ შესაძლებლობებს მიაღწიოს, რომ ადამიანზე ძლიერი სუპერ ხელოვნური ინტელექტი შექმნას. ეს კი იმის საშიშროებას გააჩენს, რომ სუპერ ხელოვნურმა ინტელექტმა თავის უსაზღვრო ცოდნა ძალაუფლების მოსაპოვებლად გამოიყენოს და გაანადგუროს მისი მეტოქე – ადამიანი. ამ სიუჟეტზე არაერთი ფანტასტიკური ჟანრის ფილმია გადაღებული. საუკეთესო მაგალითად შეიძლება ჩაითვალოს ცნობილი ჰოლივუდელი რეჟისორების ჯეიმს კამერონის ფილმები „ტერმინატორი“ და სტივენ სპილბერგის „ხელოვნური ინტელექტი“.

როგორც აღინიშნა, დღეის მდგომარეობით ხელოვნური ინტელექტი მხოლოდ განვითარების პირველ ფაზაშია და გულისხმობს ვიწრო ხელოვნურ ინტელექტის (Narrow Artificial Intelligence – NAI) ცალკეულ უნარებს, სწრაფად გააანალიზოს დიდი მოცულობის ინფორმაცია.

დღეის მდგომარეობით კომპიუტერული მეცნიერებები ეყრდნობა სამ ძირითად კონცეფციას, რომლებითაც ვიწრო ხელოვნურ ინტელექტს ავითარებენ. თითოეული მათგანი ხელოვნურ ინტელექტს აძლევს სწავლის ახალ მეთოდოლოგიას, რაც ეხმარება მათ სრულყოფაში.

მანქანური სწავლება (Machine Learning), რომლის დროსაც პროგრამა იღებს საცდელი მაგალითების წარმოუდგენლად დიდ რაოდენობას კონკრეტული დავალებების შესასრულებლად. როგორც კომპიუტერი, ის არ ჩერდება, ამუშავებს, სწავლობს და აანალიზებს, ახდენს ახალი სტრატეგიის ადაპტირებას კონკრეტული ობიექტების იდენტიფიცირებისთვის. მაგალითად, სურათის ამოცნობა, როდესაც ერთი და იგივე სახეობის ნივთის ან საგნის აღმნიშვნელ რამდენიმე ასეულ ფოტოს ტვირთავენ, ამუშავებინებენ და ამახსოვრებინებენ ხელოვნური ინტელექტის პროგრამას.

სიღრმისეული სწავლება (Deep Learning) თუ პირველი მეთოდი პროგრამას ერთი დონის საგნებისა და ინფორმაციის დამუშავებით ზღუდავს, სიღრმისეული მეთოდის დროს კომპიუტერებს საშუალებას აძლევს, პრობლემები სხვა დონეებსა და სფეროში გადაჭრას. მაგ, პროგრამამ, რომელმაც ისწავლა, მაგალითად, ვაშლის მსხლისგან გარჩევა, ეს ცოდნა შეიძლება გამოიყენოს

სხვა „პატერნებისა“[59] და კატეგორიების იდენტიფიცირებისთვის ბევრად უფრო რთულ გრაფიკებში.

ნეირონული ქსელები (Neuronal Network) ხელოვნური ნეირონული ქსელების შთაგონებად ადამიანის ტვინში არსებული ნეირონული ქსელები იქცა. მეცნიერებმა ადამიანის ტვინის მოდელი ხელოვნური ქსელების შესაქმნელად გამოიყენეს. ნეირონული ქსელების მოდელები მათემატიკური და კომპიუტერული მოდელების გამოყენებით ხელოვნურ ინტელექტს ბევრად მეტი ინფორმაციის აღქმისა და გაანალიზების უნარს აძლევს. მაგრამ ადამიანის ნეირონული ქსელებისგან განსხვავებით, რომლებიც თავის ტვინშია „ჩაშენებული“, ხელოვნური ინტელექტის პროგრამები პროგრამულ კოდებს იყენებენ. საოცარია ის ფაქტი, რომ ხელოვნური ნეირონული ქსელების მუშაობის პრინციპი ადამიანის ნეირონული ქსელის მუშაობის მოდელს ეყრდნობა.

ხელოვნური ინტელექტის გამოყენება ელექტრონულ მმართველობაში მისი წარმოუდგენლად დიდი შესაძლებლობების გამო საჯარო სამსახურებს საშუალებას მისცემს, თავიანთი საქმიანობა ცალკეულ სფეროებში უფრო ეფექტური გახადონ. უპირველესად ეს ეხება ისეთ სფეროებს, რომლებშიც მნიშვნელოვანია დიდი მონაცემების (ე.წ. Big Data) გადამუშავება. ასეთი სფეროებია კი მრავლადაა, თუმცა საქართველოსთვის პრიორიტეტად შეიძლება გამოიყოს ჯანდაცვის, აგრარული, განათლებისა და იუსტიციის სფეროები.

იმისათვის, რომ საქართველომ ზუსტად განსაზღვროს ელექტრონული მმართველობის სფეროში ხელოვნური ინტელექტის გამოყენების ცალკეულ სფეროთა პრიორიტეტულობა, აუცილებელია შემუშავებულ იქნეს ხელოვნური ინტელექტის განვითარების ეროვნული სტრატეგია. სტრატეგია განსაზღვრავს, ქვეყნის მოკლევადიან და საშუალოვადიან პერსპექტივაში რომელ სფეროებში იქნება შესაძლებელი ელექტრონული მმართველობის პირობებში ხელოვნური ინტელექტის გამოყენება[60]. ამგვარი სტრატეგიები არაერთ ქვეყანას აქვს უკვე შემუშავებული[61].

დღეის მდგომარეობით ხელოვნურ ინტელექტს იყენებს სახელმწიფო ინსტიტუტების მხოლოდ მცირე ნაწილი, ძირითადად სამართალდამცავი ორგანოები (შინაგან საქმეთა სამინისტრო ვიდეოსამეთვალყურეო სისტემების მეშვეობით სამართალდარღვევათა იდენტიფიცირებისა და გაანალიზებისთვის), ასევე ეკონომიკის სფეროში სსიპ – ტურიზმის ეროვნული ადმინისტრაცია – „სენტიმენტების ავტომატური ანალიზი“ („Emotions Are Georgia“) და განათლების სფეროში – სსიპ განათლების მართვის საინფორმაციო სისტემა – „მონა-

[59] პატერნი (ინგ. pattern) – ნიმუში, მოდელი, მსგავსება.

[60] იხ. PMCG-ის კვლევა – საქართველო – მზად ხელოვნური ინტელექტის ეპოქისთვის? 2021, https://pmcg-i.com/news_show/622/Sharing-the-Results-of-Our-Research-on-Georgia%E2%80%99s-Artificial-Intelligence-(AI)-Readiness (ბოლო ნახვის თარიღი 28.03.2021)

[61] იხ. ბიზნესისა და ტექნოლოგიების უნივერსიტეტის კვლევა – – ხელოვნური ინტელექტის ეროვნული სტრატეგიის განვითარების საჭიროება საქართველოში (კვლ. ხელმ. ნ. ენუქიძე, მ. დგებუაძე), 2020, https://btu.edu.ge/ka/kvlevebi/kvlevis-angarishebi (ბოლო ნახვის თარიღი 28.03.2021)

ცემთა ასოციაციური ანალიზი“, სსიპ – განათლების ხარისხის განვითარების ეროვნული ცენტრი – „DLP და მთარგმნელობითი მეხსიერების მოდული“)[62].

სამწუხაროდ, დღეის მდგომარეობით ხელოვნური ინტელექტი არ გამოიყენება ჯანდაცვის სფეროში, რომელშიც აუცილებელია დიდი მონაცემების სწრაფი გაანალიზება როგორც ზუსტი დიაგნოსტიკისთვის, ასევე პანდემიის წინააღმდეგ აქტიურად საბრძოლველად. ამის საუკეთესო მაგალითებია სამხრეთ კორეა და ჩინეთი, რომლებიც ეფექტურად იყენებენ ხელოვნურ ინტელექტს როგორც პანდემიის წინააღმდეგ ბრძოლისათვის, ასევე დაავადებათა დიაგნოსტიკის, ანალიზისა და მკურნალობის ნაწილში.

ასევე ძალიან მნიშვნელოვანია ხელოვნური ინტელექტის გამოყენება აგრარულ სფეროში. როგორც ცნობილია, საქართველოს მოსახლეობის თითქმის ნახევარი დღეის მდგომარეობით აგრარულ სექტორშია დასაქმებული. აქ სახელმწიფო სუბსიდირების რამდენიმე მნიშვნელოვანი პროგრამა არსებობს, რომელთა მონიტორინგისა და ანალიზისათვის ხელოვნური ინტელექტის პროგრამების დანერგვა დარგის მენეჯმენტს გაცილებით ეფექტურად აქცევს. ამის საუკეთესო მაგალითია ესტონეთი და ისრაელი, სადაც დრონებისა და ხელოვნური ინტელექტის პროგრამების გამოყენებით ხდება სახელმწიფო პროგრამებით სუბსიდირებული პროგრამების მონიტორინგი, ანალიზი და პრიორიტეტული მიმართულებების დადგენა.

ღია მონაცემების ერთიანი პორტალები

1970-იანი წლებიდან პერიოდს ინფორმაციული ერის დასაწყისს უწოდებენ, ხოლო სიტყვათშეთანხმება „ღია მონაცემების“ გამოყენება ადრეული 1980-იანი წლებიდან იწყება. ელექტრონული დემოკრატიის, ისე როგორც ზოგადად დემოკრატიის ერთ-ერთი ქვაკუთხედია ხელისუფლების გამჭვირვალობა, რადგან მხოლოდ ურთიერთნდობასა და ხელისუფლების ანგარიშვალდებულებაზე დაფუძნებულ საზოგადოებას შესწევს დემოკრატიულ პრინციპებზე დაფუძნებული სახელმწიფოს მართვის ძალა. აღსანიშნავია, რომ ელექტრონული მმართველობის კონცეფცია, მისი თავდაპირველი სახით, ნაკლებ ყურადღებას უთმობდა ელექტრონული გამჭვირვალობის კომპონენტის განვითარებას, ვინაიდან ორიენტირებული იყო ელექტრონული მომსახურების გაწევით ადმინისტრაციული ხარჯების შემცირებასა და მმართველობის ეფექტიანობის ხარისხის გაუმჯობესებაზე. ამის ერთ-ერთი მიზეზი შესაბამისი საკანონმდებლო ნორმების/რეგულაციების არარსებობაც იყო, რაც ელექტრონული გამჭვირვალობის დამკვიდრებისთვის აუცილებელ სამართლებრივ ბაზას შექმნიდა. თუმცა, 2008 წელს დაწყებულმა მსოფლიო ეკონომიკურმა კრიზისმა ამ მხრივ ბევრი რამ

[62] იხ. ხელოვნური ინტელექტის სისტემის გამოყენება საქართველოში. კანონმდებლობა და პრაქტიკა, IDFI-ს კვლევა, თბ. 2021, გვ. 8 იხ. https://idfi.ge/public/upload/Article/AI%20ENG%20FULL.pdf (ბოლო ნახვის თარიღი 28.03.2021)

შეცვალა. უპირველეს ყოვლისა, ეს ცვლილებები გამოწვეული იყო ბიზნეს და სახელმწიფო სექტორისადმი საზოგადოების ნდობის უპრეცედენტო ვარდნით. სწორედ გლობალური ეკონომიკური კრიზისის ფონზე წამყვანი დემოკრატიული ქვეყნები დარწმუნდნენ ელექტრონული გამჭვირვალობის ახალი სტანდარტების დამკვიდრების აუცილებლობაში. ამის ერთ-ერთი ყველაზე თანამედროვე მაგალითია აშშ-ის პრეზიდენტის ინოვაციური სტრატეგია „გამჭვირვალე და ღია მთავრობის ინიციატივა“ (Open Government Initiative).

საქართველოში ელექტრონული ჩართულობის ოთხი მთავარი სფეროა განსაზღვრული: უკუკავშირი ელექტრონულ სერვისებთან მიმართებით, ელექტრონული სერვისების შემუშავებაში ჩართულობა, ღია მონაცემები, გამჭვირვალობა, ღია მმართველობა, დაბოლოს, გადაწყვეტილების მიღება და პოლიტიკის შემუშავება.

ღია მმართველობა მრავალმხრივ ხედვას წარმოადგენს იმის შესახებ, თუ როგორ უნდა ჩამოყალიბდეს ე.წ. „ელექტრონული საზოგადოება“. ღია მმართველობის მიზანს წარმოადგენს მოქალაქეთა საყოველთაო ჩართვა ელექტრონული საზოგადოების განვითარების ყველა ასპექტში. ღიაობის მიდგომას შეიძლება სხვადასხვა საზოგადოებრივი პერსპექტივიდან შევხედოთ: საზოგადოდ ღია (ღია მონაცემები და ღია კოდი), ღია წვდომა (სამეცნიერო ნაშრომებსა და მონაცემებზე), ღია გალერეები, ბიბლიოთეკები, არქივები და მუზეუმები, ღია ინოვაციები. ღია მმართველობა ორიენტირებულია საჯარო სექტორის მიერ ღიაობის პრინციპის გამოყენებაზე.[63] ამ აზრით, ინფორმაციის ხელმისაწვდომობასა და ღია მონაცემების კონცეფციას განსაკუთრებული ადგილი უკავია ღია მმართველობის პროცესში.

ინტერნეტისა და ახალი ტექნოლოგიების განვითარებამ მნიშვნელოვანი როლი ითამაშა მთავრობების ღიაობისა და მათი საქმიანობის გამჭვირვალობის უზრუნველსაყოფად. ინოვაციურმა აპლიკაციებმა და პლატფორმებმა შესაძლებლობა მისცეს დაწესებულებებს, რომ უკეთ გაეგოთ საზოგადოების მოთხოვნები და საჭიროებები. მოქალაქეებს გაუჩნდათ ბერკეტი, რომ მონაწილეობა მიიღონ გადაწყვეტილებების მიღების პროცესში, ფართო საზოგადოებას გაუზიარონ საკუთარი იდეები და აღასრულონ ისინი.

ინფორმაციის თავისუფლება და ღია სამთავრობო მონაცემები

ინფორმაციის თავისუფლება ღია მმართველობის ერთ-ერთი უმნიშვნელოვანესი ფაქტორია. მისი არსის გასარკვევად მნიშვნელოვანია მთელი რიგი ცნებებისა და ინსტიტუტების განმარტება, რომლებიც მოცემულია საქართველოს ზოგადი ადმინისტრაციული კოდექსის (სზაკ) მე-3 თავში. პირველ რიგში, უნდა გავითვალისწინოთ, რომ ინფორმაციის თავისუფლება გულისხმობს საჯარო დაწესებულებებში დაცულ საჯარო ინფორმაციაზე ხელმისაწვდომობას.

[63] ციფრული საქართველო – ელექტრონული საქართველოს სტრატეგია 2014-2018 წ.წ.

სზაკ-ი ადგენს საჯარო დაწესებულებაში არსებული ინფორმაციის საჯაროობის პრეზუმფციას და მისი განმარტებისთვის გამოიყენება ნეგატიური დათქმა, რომლის თანახმადაც საჯარო დაწესებულებაში არსებული ნებისმიერი ინფორმაცია, რომელიც არ მიეკუთვნება პერსონალურ მონაცემებს, სახელმწიფო ან კომერციულ საიდუმლოებას, არის საჯარო.

სზაკ-ის მე-2 მუხლის პირველი ნაწილის „მ“ ქვეპუნქტის თანახმად, საჯარო ინფორმაცია არის: ოფიციალური დოკუმენტი (მათ შორის, ნახაზი, მაკეტი, გეგმა, სქემა, ფოტოსურათი, ელექტრონული ინფორმაცია, ვიდეო- და აუდიოჩანაწერები) ანუ საჯარო დაწესებულებაში დაცული, აგრეთვე საჯარო დაწესებულების ან მოსამსახურის მიერ სამსახურებრივ საქმიანობასთან დაკავშირებით მიღებული, დამუშავებული, შექმნილი ან გაგზავნილი ინფორმაცია, ასევე საჯარო დაწესებულების მიერ პროაქტიულად გამოქვეყნებული ინფორმაცია. რაც შეეხება მისი შინაარსის განსაზღვრის კრიტერიუმებს, ის კოდექსში არ არის მოცემული. კანონმდებლის ასეთი მიდგომა მიუთითებს იმ გარემოებაზე, რომ საჯარო ინფორმაციის ცნება არ საჭიროებს სპეციალურ განმარტებას, რამდენადაც საჯარო დაწესებულებაში (ლეგალურ დეფინიციაში მოცემული ფორმით) არსებული ნებისმიერი ინფორმაცია არის საჯარო, თუ ის არ მიეკუთვნება კონფიდენციალურ ინფორმაციათა რომელიმე სახეს.

ინფორმაციის ხელმისაწვდომობა უკავშირდება საჯარო მმართველობის განხორციელების პროცესს. ამ პროცესის გამჭვირვალობისთვის აუცილებელია, სამსახურებრივ საქმიანობასთან დაკავშირებით მიღებული, დამუშავებული, შექმნილი ან გაგზავნილი ინფორმაცია ყველასათვის ხელმისაწვდომი იყოს.

ინფორმაციის ღიაობა აქტუალური ხდება მაშინაც, როცა სუბიექტი მმართველობით ფუნქციას არ ასრულებს, მაგრამ მისი საქმიანობა ხორციელდება სახელმწიფო ან ადგილობრივი თვითმმართველობის ბიუჯეტის სახსრებიდან დაფინანსების ფარგლებში.

ინფორმაციის თავისუფლების მიზნებისთვის სზაკ-ით განისაზღვრა, რომ სუბიექტი, რომელიც ახორციელებს საჯარო სამართლებრივ უფლებამოსილებებს (ადმინისტრაციული ორგანო) ან მოქმედებს სახელმწიფო ან ადგილობრივი თვითმმართველობის დაფინანსების ფარგლებში, საჯარო დაწესებულებაა და მასზე ვრცელდება ინფორმაციის ხელმისაწვდომობის მოთხოვნა.

ამავე კოდექსისა და ასევე საქართველოს კონსტიტუციის მე-18 მუხლის მიხედვით, ყველას აქვს უფლება, კანონით დადგენილი წესით გაეცნოს საჯარო დაწესებულებაში არსებულ ინფორმაციას ან ოფიციალურ დოკუმენტს, გარდა იმ შემთხვევისა, როდესაც იგი შეიცავს კომერციულ ან პროფესიულ საიდუმლოებას, ან დემოკრატიულ საზოგადოებაში აუცილებელი სახელმწიფო ან საზოგადოებრივი უსაფრთხოების, ანაც სამართალწარმოების ინტერესების დასაცავად კანონით ან კანონით დადგენილი წესით აღიარებულია სახელმწიფო საიდუმლოებად.

საჯარო დაწესებულება ვალდებულია, გასცეს საჯარო ინფორმაცია, მათ შორის, ელექტრონული ფორმით მოთხოვნილი საჯარო ინფორმაცია, დაუყოვნებლივ ან არაუგვიანეს 10 დღისა, თუ საჯარო ინფორმაციის მოთხოვნაზე პასუხის გაცემა მოითხოვს: ა) სხვა დასახლებულ პუნქტში არსებული მისი სტრუქტურული ქვედანაყოფიდან ან სხვა საჯარო დაწესებულებიდან ინფორმაციის მოძიებასა და დამუშავებას; ბ) მნიშვნელოვანი მოცულობის ერთმანეთთან დაუკავშირებელი ცალკეული დოკუმენტების მოძიებასა და დამუშავებას; გ) სხვა დასახლებულ პუნქტში არსებულ მის სტრუქტურულ ქვედანაყოფთან ან სხვა საჯარო დაწესებულებასთან კონსულტაციას.

ღია მონაცემები

რაც შეეხება ღია მონაცემს, საჯარო დაწესებულებებისთვის ეს უკანასკნელი წარმოადგენს ელექტრონულ ფორმატში სტრუქტურირებული სახით არსებულ ისეთ მონაცემს, რომლის გასაჯაროება დასაშვებია და გამოქვეყნება მარტივადაა შესაძლებელი. სხვა სიტყვებით რომ ვთქვათ, ღია მონაცემები საჯარო ინფორმაციის იმ ნაწილს წარმოადგენს, რომლებიც საჯაროდ ხელმისაწვდომია იმგვარად, რომ შესაძლებელია მათი ხელმეორედ, მათ შორის, სხვა მიზნით გამოყენება. მაგ. საჯაროა ინფორმაცია ავტორიზებული საგანმანათლებლო დაწესებულებების შესახებ. ჩვეულებრივ, ეს გულისხმობს ცალკეული დაწესებულების შესახებ ინფორმაციის მოპოვების შესაძლებლობას, ხოლო ღია მონაცემების ფორმატში ამ ინფორმაციის გამოქვეყნება გულისხმობს შესაძლებლობას, რომ ამ მონაცემების დამუშავებით დაინტერესებულმა გააანალიზოს მონაცემები და შექმნას მათი ვიზუალიზაცია წლების მიხედვით ავტორიზაციის შესახებ გადაწყვეტილების მიღების თაობაზე ან ამ დაწესებულებათა გეოგრაფიული ადგილმდებარეობის შესახებ და ა.შ.

საქართველოს კანონმდებლობით არ არის დადგენილი ღია მონაცემების გამოქვეყნების სპეციალური ვალდებულება საჯარო დაწესებულებებისთვის. ასევე არ არის განსაზღვრული ღია მონაცემების სტანდარტები და გამოქვეყნების წესი. შესაბამისად, პორტალზე ღია მონაცემების გამოქვეყნება სრულად დამოკიდებულია საჯარო დაწესებულების ხელმძღვანელთა კეთილ ნებაზე.

საჯარო დაწესებულებები ყველგან და მათ შორის, საქართველოშიც როგორც ცენტრალურ, ასევე ადგილობრივ დონეზე ყოველდღიურ რეჟიმში ამუშავებენ ღია მონაცემებს.

ღია მონაცემების რეგულარულად და სათანადო ფორმით გამოქვეყნება შესაძლებლობას აძლევს მოქალაქეებს, ბიზნესსექტორსა და ნებისმიერ დაინტერესებულ პირს, გაეცნოს სახელმწიფო მონაცემებს და მათი გამოყენებით შექმნას ინოვაციური აპლიკაციები, ბიზნესპროექტები და ელექტრონული სერვისები.

ღია მონაცემების პრინციპები

ღია მონაცემების თემაზე მომუშავე სხვადასხვა ავტორიტეტული ორგანიზაციის მიერ სხვადასხვა წყაროში მითითებულია ამ მონაცემთა შემდეგი პრინციპები:

სისრულე – გამოქვეყნებული მონაცემები უნდა იყოს შეძლებისდაგვარად სრული და საკითხს ყოვლისმომცველად ასახავდეს.

პირვანდელობა – ღია მონაცემები პირველწყაროს მიხედვით უნდა იყოს წარმოდგენილი, რაც მათ უტყუარობას უზრუნველყოფს. სხვა შემთხვევაში, მნიშვნელოვანია, მომხმარებელს ჰქონდეს საშუალება გადაამოწმოს, რამდენად სწორადაა მონაცემები აგრეგირებული, რისთვისაც საჭიროა მეტამონაცემები (მონაცემთა ბაზის ზოგადი აღწერა), რომელიც, სხვა მახასიათებლებთან ერთად, განმარტავს, თუ როგორ შეიქმნა და დამუშავდა მონაცემები.

დროულობა – გამოქვეყნებული მონაცემები საზოგადოებისთვის დროულად უნდა იყოს ხელმისაწვდომი. მნიშვნელოვანია, შეგროვებული და დამუშავებული ოფიციალური მონაცემები მყისიერად გავრცელდეს და გამოქვეყნებისას მონაცემი კვლავაც ღირებული იყოს.

ხელმისაწვდომობა – მონაცემებზე წვდომა მარტივი უნდა იყოს. შესაბამისად, მომხმარებელს არ უნდა უწევდეს მონაცემებისთვის რომელიმე საჯარო დაწესებულებაში მისვლა. ელექტრონული ხელმისაწვდომობის თვალსაზრისით, სასურველია, რომ მონაცემები თავმოყრილი იყოს ცენტრალურ პლატფორმაზე/ერთ ადგილას. ასევე, შესაძლებელი უნდა იყოს მონაცემების გადმოწერა.

დამუშავებადი / მანქანა-კითხვადი (Machine readable) ფორმატი – მონაცემი სტრუქტურირებული უნდა იყოს ისე, რომ შესაძლებელი იყოს სხვადასხვა მიზნით მისი ავტომატური დამუშავება.

არაექსკლუზიურობა – მონაცემები ხელმისაწვდომი უნდა იყოს ისეთ ფორმატში, რომელზეც არავის არ ექნება ექსკლუზიური განკარგვის უფლება. ამიტომ სასურველია, მონაცემები ხელმისაწვდომი იყოს რაც შეიძლება მეტ სხვადასხვა ფორმატში. ამით არავის ექნება საშუალება, დააწესოს გარკვეული შეზღუდვები მონაცემების გამოყენებასა და გაზიარებაზე.

ლიცენზიისგან თავისუფალი – მონაცემებზე არ უნდა ვრცელდებოდეს რაიმე სახის ინტელექტუალური და საავტორო უფლებების რეგულაციები. დასაშვებია მხოლოდ პერსონალურ მონაცემებთან და უსაფრთხოებასთან დაკავშირებული შეზღუდვების დაწესება.

შემოწმება – ყველა დაწესებულებამ უნდა განსაზღვროს პირი, რომელიც პასუხისმგებელი იქნება ღია მონაცემების თაობაზე მოქალაქეებთან კომუნიკაციაზე. ამ პირის შესახებ ინფორმაცია ხელმისაწვდომი უნდა იყოს ღია მონაცემების პორტალზე.

ძებნა – მონაცემების პოვნა იოლად უნდა იყოს შესაძლებელი. ძებნის ველები მომხმარებლის საჭიროებებზე უნდა იყოს მორგებული.

მუდმივობა – ღია მონაცემებზე წვდომა განუსაზღვრელი დროით უნდა იყოს შენარჩუნებული. ამისთვის, მნიშვნელოვანია კონკრეტულ ვებმისამართზე გამოქვეყნებული მონაცემი რაც შეიძლება დიდხანს იყოს განთავსებული, რათა მომხმარებელმა ინფორმაცია წყაროს მითითებით გაავრცელოს. საჭიროების შემთხვევაში უნდა შეიქმნას ღია მონაცემების არქივი.

არადისკრიმინაციულობა – მონაცემები ხელმისაწვდომი უნდა იყოს ყველასთვის. მათ გასაცნობად საჭირო არ უნდა იყოს რეგისტრაცია, რაც გულისხმობს პირის იდენტიფიცირებას, რათა მონაცემებზე წვდომის ნებართვის პროცესში პირთა დისკრიმინაცია გამოირიცხოს.

განახლებადი – დაწესებულებებმა უნდა უზრუნველყონ მონაცემების მუდმივი განახლება.

ღია მონაცემების პორტალები საქართველოში

2011 წლის სექტემბერში საქართველოს მთავრობა შეუერთდა ღია მმართველობის პარტნიორობის შეთანხმებას და წარადგინა 2012-2013 წლების სამოქმედო გეგმა შემდეგი მიზნით: „მთავრობა გახდება უფრო გამჭვირვალე, ანგარიშვალდებული, ინოვაციური და ღია მოქალაქეთა ჩართულობისათვის".[64] ღია მონაცემების რეგულარულად და ეფექტიანად გამოქვეყნების მიზნით, ღია მმართველობა საქართველოს 2014-2015 წლების სამოქმედო გეგმის ფარგლებში, იუსტიციის სამინისტროს საჯარო სამართლის იურიდიული პირის „მონაცემთა გაცვლის სააგენტოს" მიერ შეიქმნა ღია მონაცემთა პორტალი www.data.gov.ge. პორტალის შექმნიდან დღემდე მასზე მონაცემების განთავსება დაბალი სიხშირითა და ინტენსივობით ხდება, განსაკუთრებით კი ადგილობრივი ხელისუფლების მხრიდან. პორტალი უზრუნველყოფს სახელმწიფო დაწესებულებების ღია მონაცემების გამოქვეყნებას ღია, გამოთვლად და ყველასთვის ხელმისაწვდომ ფორმატებში, რაც მოქალაქეებს, ბიზნესს, მასმედიის წარმომადგენლებს, არასამთავრობო და სამთავრობო დაწესებულებებს საშუალებას მისცემს, შეუფერხებლად ისარგებლონ აღნიშნული მონაცემებით, მათი გამოყენებით შექმნან აპლიკაციები და ელექტრონული სერვისები და მიიღონ სხვა სახის სარგებელი. პორტალზე გამოქვეყნებული მონაცემთა ცხრილები წარმოდგენილია ღია მონაცემების სტანდარტულ ფორმატებში (CSV ან XML). მონაცემები ასევე შეიძლება ხელმისაწვდომი იყოს ელექტრონული სერვისის საშუალებით (API). მონაცემები დაჯგუფებულია როგორც ორგანიზაციებს მიხედვით, ისე თემატურად.

სახელმწიფო შესყიდვების სააგენტო, მსოფლიო ბანკისა და საერთაშორისო განვითარების დეპარტამენტის (Department of International Development – DFID) მხარდაჭერით, ასევე ღია მონაცემთა პარტნიორობასთან (Open Contracting Partnership – OCP) თანამშრომლობით აქტიურად მუშაობს Open Contracting Data Standard (OCDS)-ის დანერგვაზე. აღსანიშნავია, რომ OCDS გულისხმობს ღია მონაცემთა პუბლიკაციის სტანდარტის შემოღებას, რომელიც უზრუნველყოფს სატენდერო ინფორმაციისა და ხელშეკრულების შესრულების ყველა ეტაპზე (დაგეგმარებიდან განხორციელებამდე) სტრუქტურიზებული ინფორმაციის გამოქვეყნებას. ამ ეტაპზე, დასრულებულია OCDS-ის დანერგვის პირველი ეტაპის სამუშა-

[64] ციფრული საქართველო – ელექტრონული საქართველოს სტრატეგია 2014-2018 წ.წ.

ოები, რაც გულისხმობს როგორც აგრეგირებული, ასევე ცალკეულ შესყიდვებზე არსებული ინფორმაციის სპეციალურ წაკითხვად (Machine readable) ფორმატში (JSON) სისტემატურ გამოქვეყნებას საგანგებოდ შექმნილ ვებგვერდზე – http://opendata.spa.ge.

საქართველოს გარემოს დაცვისა და სოფლის მეურნეობის სამინისტროს ღია მონაცემთა პორტალი ხელმისაწვდომია ბმულზე http://data.mepa.gov.ge.

გარდა სახელმწიფო დაწესებულებებისა, ერთ-ერთი ა(ა)იპ-ის მიერ შექმნილია ღია მონაცემების პორტალი https://www.datalab.ge, რომელზეც, გარდა მონაცემებისა, ზოგიერთ შემთხვევაში ხელმისაწვდომია მონაცემთა ცალკეულ ჭრილში ვიზუალიზაციის დოკუმენტებიც.[65]

მსოფლიოში არსებობს ღია მონაცემებზე დაფუძნებული პროდუქტებისა და მომსახურებების უამრავი მაგალითი. სამაგალითოდ იხ. რამდენიმე ცნობილი პორტალის მისამართი:

https://openspending.org/ – დიდ ბრიტანეთში შექმნილი პორტალი, რომელზეც ხდება მონაცემთა ვიზუალიზაცია და ინფორმაცია მარტივი ფორმით მიეწოდება მომხმარებელს; დაფუძნებულია ფინანსური ხასიათის ღია მონაცემებზე;

London Traffic – ბრიტანეთი: სატრანსპორტო საშუალებების გზებზე გადატვირთულობა; მონაცემთა წყარო: ქალაქში დამონტაჟებული კამერები და პოლიციის მონაცემები;

London Fire Brigade – ბრიტანეთი. გამოძახებების რაოდენობა რაიონების მიხედვით; ადგილზე მისვლის დრო. მონაცემების მიხედვით იგეგმება: სამაშველო ბრიგადების განლაგება/აღჭურვა, რეგულარული შემოწმებები, ხალხის ინფორმირება, სპეციალური მოწყობილობების განლაგება;

GoodSAM – ლონდონი;

PulsePoint – მობილური აპლიკაცია, რომლის დახმარებითაც შეუძლოდ გახდომის შემთხვევაში ადამიანები ატყობინებენ სასწრაფოსა და გარშემომყოფებს.

Kannattaako Kauppa – ფინეთი. ბინების ფასების პროგნოზირება.

RomaScoula – იტალია. საგანმანათლებლო დაწესებულებების შეფასება მასწავლებლების მოსწრების, ინტერნეტის ხელმისაწვდომობის, IT მოწყობილობების, განათლების ხარისხის, გაცემული დიპლომებისა და სხვა ინდიკატორების მიხედვით.

Carambla – Park Smart – ბელგია. მანქანის გასაჩერებელი ადგილის მოძებნა, დაჯავშნა და გადახდა.

[65] იხ. რამდენიმე სასარგებლო ბმული: www.ckan.org/about/ – ღია პროგრამა მონაცემთა პლატფორმების შესაქმნელად; https://data.europa.eu/euodp/en/home – ევროკავშირის ღია მონაცემების პორტალი; https://www.europeandataportal.eu/en – ევროპის ღია მონაცემების პორტალი; http://data.gouv.fr – საფრანგეთის ღია მონაცემების პორტალი;https://data.gov.ie – ირლანდიის ღია მონაცემების პორტალი; www.data.gov/ – აშშ-ის ღია მონაცემების პორტალი; www.open.canada.ca/en – კანადის ღია მონაცემების პორტალი; www.data.gov.au – ავსტრალიის ღია მონაცემების პორტალი.

Rejestr.io – პოლონეთი. პორტალი უზრუნველყოფს მარტივ და უფასო წვდომას მრავალრიცხოვან ღია მონაცემებზე ბიზნესის, სახელმწიფო შესყიდვებისა და სხვა უამრავი მონაცემის ჩათვლით.

Sejmometr.pl – პოლონეთი. აპლიკაცია შეიცავს ინფორმაციას პარლამენტისა და პარლამენტის წევრების მუშაობის შესახებ.

Kurtyna w Gore! – პოლონეთი. ვარშავის კულტურული ღონისძიებები. მომხმარებელს შეუძლია ღონისძიებების დამატება და ძიება.

https://www.hlidacstatu.cz/ – პოლონეთი. დასახელება „სახელმწიფოს მცველი". სახელმწიფოს მოდარაჯეები (Guardians of the State) მოიცავს რამდენიმე სერვისს: შესყიდვების მოდარაჯეები („Hlídač smluv", hlidacsmluv.cz) – თავდაპირველი და, ამავდროულად, ყველაზე მნიშვნელოვანი სერვისი – განახლებული სახით აქვეყნებს ინფორმაციას შესყიდვების რეესტრის მეშვეობით და კიდევ უფრო მეტად არის მორგებული მომხმარებელზე (უკეთესი საძიებო სისტემა და ა.შ.), ხალხის მოდარაჯეები – პოლიტიკოსებისა და პოლიტიკაში მყოფი სხვა პირების შესახებ შეგროვებული ინფორმაციის გამოსაქვეყნებლად და ა.შ.

ინფორმაციის ერთიანი რეესტრი

საჯარო სექტორში ინფორმაციული ტექნოლოგიების შეღწევის დონისა და გამოყენების ინტენსივობის გათვალისწინებით, ინფორმაციული სისტემების თანმიმდევრული და ეფექტიანი განვითარებისთვის მნიშვნელოვანია კოორდინირებული ქმედებები. წარმატებული კოორდინაციის წინაპირობას კი, თავის მხრივ, წარმოადგენს სწორი და ამომწურავი ინფორმაციის ფლობა იმ სისტემებსა და სერვისებზე, რომელთაც სახელმწიფო სულ უფრო მეტი ოდენობით სთავაზობს მოქალაქეებს და სხვა მომხმარებლებს.

ამ მიზნით 2011 წლის 1-ელ ივნისს ამოქმედდა „ინფორმაციის ერთიანი სახელმწიფო რეესტრის შესახებ" საქართველოს კანონი, რომლის მიზანია სახელმწიფო ხელისუფლების ორგანოებში მოქმედი მონაცემთა ბაზების, რეესტრების, ინფორმაციული სისტემებისა და მომსახურებების ერთიანი კატალოგის შექმნა, რომელიც სრულად აღწერს საქართველოს საჯარო სექტორში არსებულ ინფორმაციულ-ტექნოლოგიურ რესურსებს. ინფორმაციის ერთიან სახელმწიფო რეესტრში არ შედის და არ მუშავდება მონაცემები კერძო სამართლის პირთა მონაცემთა ბაზების, რეესტრების, ინფორმაციული სისტემებისა და მომსახურების შესახებ. ფაქტობრივად, ინფორმაციის ერთიანი სახელმწიფო რეესტრი არის საჯარო სექტორში არსებული ინფორმაციულ-ტექნოლოგიური რესურსების თაობაზე ინფორმაციის ერთიანობა, ამ ინფორმაციის ერთიანი კატალოგი, რომელიც, თავის მხრივ, მიზნად ისახავს საჯარო რესურსების ეფექტიანად გამოყენებას და ყველა იმ რესურსის აღწერას, რომელიც უკვე არსებობს/შექმნილია საჯარო სექტორში.

რეესტრის შექმნასა და ფუნქციონირებაზე დღეს პასუხისმგებელია საქართველოს იუსტიციის სამინისტროს სსიპ „მონაცემთა გაცვლის სააგენტო“, მათ შორის შესაბამის პროგრამულ გადაწყვეტაზე – „ინფორმაციის ერთიანი სახელმწიფო რეესტრის პორტალი“.

აღნიშნული პორტალი ფუნქციონირებს მისამართზე http://roi.gov.ge/. პორტალის მეშვეობით სახელმწიფო ხელისუფლების ორგანოებს საშუალება აქვთ, განახორციელონ საკუთარი რეესტრებისა და მომსახურებების პირველადი რეგისტრაცია, ასევე მათში მნიშვნელოვანი ცვლილებების, მათი განვრცობის, კომბინირების, გაუქმების, განადგურების, არქივირებისა და გადაცემის შეტყობინების რეგისტრაცია.

ელექტრონული პეტიციების პორტალები

პეტიცია ნიშნავს წერილობით კოლექტიურ თხოვნას, კოლექტიურ შუამდგომლობას[66], რომელიც ეგზავნება როგორც ხელისუფლების უმაღლესი ორგანოს ან მთავრობის მეთაურს, ისე სხვა პირს ან ინსტიტუციას.

ბოლო ათწლეულში მთელ მსოფლიოში დიდი პოპულარობა შეიძინა აქტივისტებისა და სხვადასხვა საინიციატივო ჯგუფების მიერ საჯარო მიმართვების, კამპანიებისა და პეტიციების გამოყენების ონლაინპრაქტიკამ.

სხვადასხვა ქვეყანაში შეიქმნა პლატფორმები, რომლებიც საშუალებას აძლევენ მოქალაქეებს, შეაგროვონ ხელმოწერები ამა თუ იმ მწვავე საკითხზე, გაავრცელონ აღნიშნული პეტიცია ან კამპანია სოციალურ მედიაში და ასევე მიაწვდინონ მოთხოვნის შინაარსი ადრესატს.

პეტიციის ადრესატები, როგორც წესი, არიან სახელმწიფო ორგანოები – როგორც ცენტრალური ხელისუფლების აღმასრულებელი (სამინისტროები, სააგენტოები) და საკანონმდებლო შტო (პარლამენტი), ასევე ადგილობრივი თვითმმართველობის ორგანოები, ზოგიერთ შემთხვევაში კი სხვადასხვა მსხვილი ბიზნესკომპანია და სხვა მსგავსი ორგანიზაციები.

საქართველოში ონლაინ პეტიციის პორტალები გააჩნიათ როგორც საქართველოს მთავრობის ადმინისტრაციას, ასევე საქართველოს პარლამენტს და ადგილობრივ თვითმმართველობებსაც.

პეტიციების ონლაინპორტალები მნიშვნელოვანია როგორც სახელმწიფო ორგანოების მხრიდან ანგარიშვალდებულების, ასევე მოქალაქეების მხრიდან საჯარო პოლიტიკის ჩამოყალიბების პროცესში ჩართულობის თვალსაზრისით.

საქართველოს მთავრობის პეტიციის პორტალი – https://ichange.gov.ge/

ღია მმართველობის პარტნიორობის (OGP) 2014 წლის მეორე სამოქმედო გეგმის ფარგლებში (საქართველოს მთავრობის 2014 წლის 18 სექტემბრის N557 დადგენილება) საქართველოს მთავრობას, კერძოდ კი საქართველოს მთავრობის ადმინისტრაციას აღებული ჰქონდა ვალდებულება, რომ ღია მმართველობის პარტნიორობის (OGP) ფუნდამენტური პრინციპების დაცვისათვის – მთავრობათა ღიაობა, გამჭვირვალობა, საზოგადოების წინაშე ანგარიშვალდებულება და გადაწყვეტილების მიღების პროცესში მოქალაქეთა ჩართულობა – შეიქმნებოდა ონლაინპეტიციების პორტალი, რომლის მეშვეობითაც გაუმჯობესდებოდა საზოგადოების ჩართულობა საჯარო პოლიტიკაში, უზრუნველყოფილი იქნებოდა

[66] ზურაბიშვილი, დ., გობრონიძე გ., სამოქალაქო განათლების ლექსიკონი, „საიას“ იურიდ. განათლ. ხელშეწყობის ფონდი, თბ., 2011. ISBN 978-9941-0-3354-4.

საქართველოს მთავრობის გადაწყვეტილებებისა და საქმიანობის გამჭვირვალობა, გაადვილდებოდა საქართველოს მთავრობისა და საზოგადოების ურთიერთდაახლოება.

ნაკისრი ვალდებულების შესაბამისად, საქართველოს მთავრობის 2017 წლის 18 მაისის №245 დადგენილებით შეიქმნა ონლაინპეტიციების პლატფორმა ichange.gov.ge და დამტკიცდა პორტალის გამოყენების წესები და პირობები.

პორტალზე პეტიციის გამოქვეყნება შეუძლია ნებისმიერ სრულწლოვან მოქალაქეს. საკითხი აუცილებლად უნდა შეეხებოდეს საქართველოს მთავრობის კომპეტენციის სფეროებს – წინააღმდეგ შემთხვევაში პეტიცია არ მიიღება.

დადგენილი წესების თანახმად, ელექტრონული პეტიციის საქართველოს მთავრობის მიერ განსახილველად და მასზე ოფიციალური პასუხის მისაღებად საჭიროა, ელექტრონულ პეტიციას მხარი დაუჭიროს არანაკლებ 10 000-მა მომხმარებელმა. 2021 წლის 1 იანვრიდან საჭირო ხელმოწერების რაოდენობა განახევრდა და დღეისათვის შეადგენს 5 000 ხელმოწერას.

პეტიციის გამოქვეყნებიდან 30 კალენდარული დღის განმავლობაში პეტიციამ უნდა დააგროვოს 5 000 ხელმოწერა, შემდეგ კი მას განიხილავს საქართველოს მთავრობის ადმინისტრაციაში შექმნილი ელექტრონული პეტიციის ექსპერტების კომისია და მომზადდება ოფიციალური პასუხი, რომელიც გამოქვეყნდება პეტიციის გვერდზე.

თუ პეტიციამ ვერ დააგროვა საჭირო რაოდენობის ხელმოწერები გამოქვეყნებიდან 30 კალენდარული დღის განმავლობაში, ჩაითვლება ვადაგასულად, გადავა არქივში და მას აღარ განიხილავენ.

ადგილობრივი თვითმმართველობების პეტიციები საქართველოში

2015 წელს საქართველოს ადგილობრივი თვითმმართველობის კოდექსში შესული ცვლილებით, 86-ე მუხლის შესაბამისად, მუნიციპალიტეტის ტერიტორიაზე რეგისტრირებული ამომრჩევლების არანაკლებ 1%-ს შეუძლია, პეტიციით მიმართოს მუნიციპალიტეტის საკრებულოს.

ამავე მუხლის 24-ე პუნქტის შესაბამისად, მუნიციპალიტეტს შეუძლია განსაზღვროს პეტიციის ელექტრონული ფორმით წარდგენის წესიც. სამწუხაროდ, ელექტრონული პლატფორმები მხოლოდ რამდენიმე მუნიციპალიტეტშია დანერგილი. პროცესი არათანაბრად ვითარდება საქართველოს სხვადასხვა რეგიონში და დღესდღეობით ქვეყნის განვითარების ყველაზე დიდი გამოწვევა კვლავ რეგიონებში არსებული ე.წ. „ციფრული უთანასწორობაა“ – ცენტრალური და ადგილობრივი ხელისუფლების დონეზე ელექტრონული მმართველობა არათანაბრად არის განვითარებული.

თბილისის მერიის ვებგვერდზე განთავსებულია მერიისათვის იდეის შეთავაზების ელექტრონული ინსტრუმენტი, რომელსაც წარმატებით იყენებენ როგორც მოქალაქეები, ისე სამოქალაქო საზოგადოებისა და არასამთავრობო ორგანიზაციების წარმომადგენლები: https://idea.municipal.gov.ge/home

საქართველოს პარლამენტის პეტიციები – HTTPS://ESIGNATURE.PARLIAMENT.GE/

საქართველოს პარლამენტის ღია პარლამენტის პროექტის ფარგლებში 2019 წელს ამოქმედდა საკანონმდებლო ინიციატივისა და პეტიციის წარდგენის ელექტრონული გვერდი, რომლის მთავარი მიზანია, უფრო უკეთ ამუშავდეს და განმტკიცდეს დემოკრატიის ისეთი მნიშვნელოვანი ინსტიტუტი, როგორიც არის სახალხო ინიციატივის უფლება – მოსახლეობისა და საზოგადოების ჩართულობა საპარლამენტო საქმიანობაში.

ელექტრონული პლატფორმა იძლევა საშუალებას, მოქალაქეებმა სამი სახის ინიციატივა შეავსონ: არანაკლებ 200 000 ამომრჩევლის ინიციატივა, არანაკლებ 25 000 ამომრჩევლის ინიციატივა და პეტიცია. ხელმოწერების შეგროვების შემდეგ ინიციატივები განსახილველად წარედგინება პარლამენტს.

პერსონალურ მონაცემთა დაცვა

პერსონალურ მონაცემთა დაცვის მნიშვნელობა ელექტრონული მმართველობის კონტექსტში

ელექტრონული მმართველობა თანამედროვე გაგებით თავისთავად გულისხმობს პერსონალური მონაცემთა ინტენსიურ დამუშავებას და პრივატულობის დაცვის რისკების ზრდას. შესაბამისად, თანამედროვე დემოკრატიულ სახელმწიფოებში ელექტრონულ მმართველობასთან დაკავშირებული ნებისმიერი ინიციატივის განხილვისას ასევე განიხილება საკითხი პერსონალურ მონაცემთა დაცვის შესახებ. სხვაგვარად რომ ვთქვათ, თავისუფალი სამყაროს ქვეყნებში, სადაც ნებისმიერი საჯარო ინიციატივა ადამიანის კეთილდღეობასა და უფლებების რეალიზაციაზეა ორიენტირებული, ელექტრონული მმართველობის ინიციატივების განუყოფელი, თანმდევი ამოცანაა პერსონალურ მონაცემთა დაცვაზე ზრუნვა.

უკანასკნელი 30 წლის განმავლობაში პერსონალურ მონაცემთა დაცვის სფეროში როგორც კანონმდებელთა, ისე იმპლემენტაციზე პასუხისმგებელ პირთა დღის წესრიგს სწორედ ციფრული ტექნოლოგიებისა და ელექტრონული მმართველობის განვითარება განაპირობებს. ამ სფეროში კანონმდებელთა თითქმის ყველა ინიციატივა და ყოველივე, რაც მონაცემთა დაცვას ემსახურება, ძირითადად ნაკარნახევია სწორედ ტექნოლოგიისა და ელექტრონული მმართველობის განვითარებით და წარმოადგენს ერთგვარ პასუხს მისგან განპირობებულ მონაცემთა დამუშავების შესაძლებლობების ზრდაზე და შესაბამის რისკებზე.

ადამიანის პერსონალურ მონაცემთა დამუშავების საკითხის რეგულირება და დაცვის ახალი საკანონმდებლო თუ ტექნოლოგიური მექანიზმების შექმნა არის საკითხი, რომელიც სულ უფრო და უფრო მზარდ მნიშვნელობას იძენს თანამედროვე მსოფლიოში. მაგალითად შეიძლება ითქვას, რომ ბოლო წლებში პერსონალურ მონაცემთა დაცვის საკითხი განიხილება ელექტრონულ მმართველობასთან დაკავშირებული ისეთი კონცეფციების კონტექსტში, როგორებიცაა ხელოვნური ინტელექტი (Artificial intelligence), თვალთვალის კაპიტალიზმი (Surveillance capitalism), მიკრო მიზანში ამოღება (Microtargeting), მონაცემებით მართული ტექნოლოგიები (Data-driven technologies) და ა.შ.

დღეისათვის ციფრული ტექნოლოგია და ელექტრონული მმართველობა საჯარო ადმინისტრირების განუყოფელი ნაწილია. უდავოა, რომ უკანასკნელი 10 წლის განმავლობაში ტექნოლოგიამ თვისებრივად შეცვალა საჯარო მმართველობა. ეს ეხება საჯარო ადმინისტრაციის საქმიანობის თითქმის ყველა ასპექტს – როგორც საჯარო დაწესებულებებს შიგნით ურთიერთობებს, გადაწყვეტილებების მომზადებისა და მიღების პროცესს, ისე მათ ინტერაქციას მოქალაქეებთან. ასევე ეჭვს არ იწვევს ის სარგებელი, რაც ელექტრონულმა მმართველობამ შეიძლება მოიტანოს საჯარო მმართველობაში – გახადოს ის უფრო ხარისხიანი, გამჭვირვალე და ხელმისაწვდომი, ვიდრე მანამდე. ელექტრონული მმართველობის დანერგვამ შესაძლებელი გახადა უფრო სწრაფი, ხელმისაწვდომი, კომფორტული

და მოქალაქეზე ორიენტირებული სერვისებს დანერგვა. თუმცა სწორედ ციფრული ტექნოლოგიების გამოყენება და ელექტრონული მმართველობა, რაც ადამიანებს ყოველდღიურ ცხოვრებას უადვილებს, პერსონალური მონაცემების ინტენსიურ დამუშავებასაც გულისხმობს, რაც პრივატულობის უფლებისადმი დამატებითი რისკების გაჩენას განაპირობებს.

ელექტრონული სერვისები რომელიც მოქალაქეებს მიეწოდებათ ან/და თავად საჯარო ადმინისტრაციის ფუნქციონირებისთვისაა საჭირო, ყოველთვის გულისხმობს მონაცემთა დამუშავების აქტივობებს, რომელშიც ერთ ან რამდენიმე ტექნოლოგია გამოიყენება, რათა უზრუნველყოფილი იქნეს უფრო მეტი ეფექტურობა, მეტი ხელმისაწვდომობა და რესურსების რაციონალური გამოყენება.

ელექტრონული მმართველობის სისტემებისთვის, ისევე როგორც ყველა ინფორმაციული სისტემისთვის, ზოგადად მონაცემებს განსაკუთრებული ღირებულება აქვს. მით უმეტეს, ელექტრონული მმართველობის თანამედროვე ინიციატივებში/მოდელებში, რომელთა ძირითადი მამოძრავებელი რესურსი და „ენერგიის წყარო“ სწორედ მონაცემებია, აშკარაა მათი მნიშვნელობა და შეუცვლელობა.

პერსონალური მონაცემების დამუშავება არის ელექტრონული მმართველობის სისტემების საფუძველი, ვინაიდან ის იძლევა მომხმარებლის იდენტიფიცირებისა და უნიკალური იდეტიფიკატორების მინიჭების შესაძლებლობას. მომხმარებლის უნიკალური იდენტიფიცირება კი სწორედ ისაა, რაც უზრუნველყოფს მოქალაქეთათვის ისეთი ელექტრონული საჯარო სერვისების ხელმისაწვდომობას, როგორებიცაა გადასახადების გადახდა, ჯარიმების გადახდა, ქონებისა და ბიზნესის რეგისტრაცია, სხვადასხვა სოციალური პროგრამით სარგებლობა და ა.შ. მოქალაქეთა პერსონალური მონაცემების დამუშავების გარეშე ცხადია, ელექტრონული მმართველობის სისტემებს არ შეუძლია სრულფასოვნად იფუნქციონიროს და მათ მაქსიმალური პოტენციალი იქნეს გამოყენებული.

ყოველივე ზემოაღნიშნულის გათვალისწინებით, ელექტრონული მმართველობის განვითარება, რაც გულისხმობს მრავალი მოქალაქის შესახებ დიდი მოცულობით მონაცემების შეგროვებას და ტექნიკური თვალსაზრისით მაღალ ხელმისაწვდომობას, განაპირობებს დამატებითი რისკებს გაჩენას პერსონალურ მონაცემთა დაცვის თვალსაზრისით. სწორედ ციფრული ტექნოლოგიისა და ელექტრონული მმართველობის მეშვეობით შეიძინა კაცობრიობის ისტორიაში აქამდე წარმოუდგენელი მასშტაბები ადამიანის შესახებ ინფორმაციის შეგროვებამ და გავრცელებამ – აქამდე არასოდეს ყოფილა შესაძლებელი, რომ ამდენ ადამიანს სცოდნოდა ჩვენზე – ჩვენი გემოვნების, სურვილების, ჯანმრთელობის, ფინანსებისა და საიდუმლოებების შესახებ. ამავე დროს, აქამდე ძნელი წარმოსადგენი იყო, რომ ადამიანს, რომელიც ჩვენგან ათეული ან ასეული კილომეტრის დაშორებით ზის კომპიუტერთან, შეიძლებოდა სხვისთვის ამხელა დახმარება გაეწია ან ამხელა ზიანი მიეყენებინა.

ისიც უნდა აღინიშნოს, რომ ელექტრონული მმართველობის კონტექსტში პერსონალური მონაცემების დამუშავება რამდენიმე თავისებურებით ხასიათდება, რაც მას კერძო სექტორში არსებული მონაცემთა დამუშავების სისტემებისგან განასხვავებს. ელექტრონული მმართველობა გულისხმობს პერსონალურ მონაცემთა დამუშავებას მოქალაქეთა ფართო წრის – მონაცემთა სუბიექტების მრავალი კატეგორიის შესახებ. უფრო მეტიც, იმ ქვეყნებში, რომლებშიც სამოქალაქო სტატუსის რეგისტრაციისა და მოსახლეობის ელექტრონული რეესტრები არსებობს, სადაც საგადასახადო, სოციალური დაცვისა და საპენსიო სისტემები ელექტრონულია, ელმმართველობა უკლებლივ ყველა მოქალაქის შესახებ ციფრული მონაცემების დამუშავებას ნიშნავს. კერძო სექტორისგან მთავარი განსხვავება ისაა, რომ მოქალაქეს, როგორც წესი, ფაქტობრივად არ აქვს შესაძლებლობა, თავად გააკეთოს არჩევანი, თუ ვინ დაამუშავებს მის მონაცემებს ან/და იყოს თუ არა ამ სისტემების ნაწილი. ელმმართველობის მიზნებისთვის საჯარო სექტორში მონაცემთა დამუშავების კიდევ ერთი თავისებურებაა ძალაუფლების დისბალანსია მონაცემთა დამმუშავებელსა და მონაცემთა სუბიექტებს შორის. სწორედ აღნიშნული გარემოებები ხდის აქტუალურს პერსონალური მონაცემების დაცვის საკითხს ელექტრონული მმართველობისას და კანონმდებლებს და პასუხისმგებელ პირებს მონაცემთა დაცვის ზრუნვისკენ მოუწოდებს.

პერსონალური მონაცემების დაცვა და დღეისათვის ამ სფეროში არსებულ რისკებთან გამკლავება მარტივი ამოცანა არაა. მით უმეტეს, იმ პირობებში როდესაც ელექტრონულ მმართველობასა თუ ელექტრონულ კომერციაში ლამის ყოველდღიურად ახალ-ახალი ტექნოლოგიები და ბიზნესმოდელები ინერგება და ძალიან მაღალია მეტი მონაცემის შეგროვების ფინანსური მოტივაცია. სწორედ ამიტომ მსოფლიოს სხვადასხვა ნაწილში კანონმდებლებს, იურისტებს, უფლებადამცველებსა თუ ტექნოლოგიის ექსპერტებს ყოველდღიურად უწევთ ზრუნვა მონაცემთა დაცვისკენ მიმართული რეგულაციებისა და ტექნოლოგიების შემუშავებასა და დანერგვაზე. შესაბამისად, საკანონმდებლო მოთხოვნები და მათგან მომდინარე ორგანიზაციულ-ტექნიკური გადაწყვეტები, რომლებიც პერსონალურ მონაცემთა დასაცავად არის რეკომენდებული, ასევე ეტაპობრივად რთულდება.

ამ ყოველივეს გათვალისწინებით, საქართველოში საჯარო ადმინისტრირების სხვადასხვა საფეხურზე მომუშავეებში ხშირად შეიმჩნევა ერთგვარი უკმაყოფილება და გაკვირვება, როდესაც პერსონალურ მონაცემთა დაცვის უზრუნველსაყოფად საჭირო სამუშაოებზე იწყება საუბარი. წუხილს ძირითადად იწვევს საკითხი, თუ რა აუცილებელია ამდენი რესურსის გაღება პერსონალურ მონაცემთა დასაცავად, რისთვისაა საჭირო საკითხის ასეთი რთული რეგულირება, ამდენი წვრილმანის გათვალისწინება და არცთუ იაფი ტექნოლოგიების გამოყენება. ზოგჯერ კი ისმის კითხვა – განა ასეთი რა სიკეთე მოაქვს პერსონალური მონაცემების დაცვას, ასეთს რას ექმნება საფრთხე, რომ ამ თემას ამდენი დრო და ენერგია დაეთმოს. მსგავსი განწყობებისა თუ კითხვების წინაპირობა ისაა, რომ მენეჯერების/მოხელეების ნაწილს ჯერ კიდევ არ აქვს გაცნობიერებული საფრთხის არსი და მნიშვნელობა. პერსონალური მონაცემების დაუცველობა მხოლოდ ცალკეული ინდივიდების შესახებ ინ-

ფორმაციის გამჟღავნებასა და მათთვის ფსიქოლოგიური დისკომფორტის მიყენებასთან ასოცირდება.

რეალურად კი პერსონალურ მონაცემთა დაცვა არ არის მხოლოდ ცალკეული ადამიანის ფსიქოლოგიური დისკომფორტისგან დაცვის საკითხი, რაც მისი მონაცემების – შემოსავლების, ვალების, ჯანმრთელობის მდგომარეობის, პირადი კავშირებისა თუ ეთნიკური წარმომავლობის – გამჟღავნებას შეიძლება მოჰყვეს შედეგად. დღეისათვის ფიზიკურ პირთა პერსონალური მონაცემების მოუწესრიგებელი და უკონტროლო დამუშავებიდან მომდინარე საფრთხეების მნიშვნელობა სცდება ადამიანისთვის მიყენებულ ფსიქოლოგიურ ზიანსა და დისკომფორტს. პერსონალურ მონაცემთა გადაჭარბებული და უკონტროლო დამუშავება ადამიანის სხვა უფლებებისა და თავისუფლებების შეზღუდვის არსებით რისკებს შეიცავს, რაც უკავშირდება ადამიანის ქცევის პროგნოზირებასა და მასზე მანიპულაციის შესაძლებლობას, ეს კი, თავის მხრივ, ასევე საფრთხეს უქმნის თანამედროვე დემოკრატიულ წესრიგს.

სხვაგვარად რომ ვთქვათ, თანამედროვე მსოფლიოში, როდესაც მონაცემთა შეგროვებისა და დამუშავების შესაძლებლობები უპრეცედენტოდ იზრდება, როდესაც ვირტუალურ სივრცეში ადამიანის მოქმედებათა კვალის აღრიცხვა ტექნიკური თვალსაზრისით ძალიან მარტივია, როდესაც ჩვენი მონაცემები და ინტერნეტში დატოვებული კვალი ჩვენივე ქცევის პროგნოზირებისა თუ კორექტირებისთვის გამოიყენება – პერსონალურ მონაცემთა დაცვა არის საკითხი, გვექნება თუ არა თავისუფალი ადამიანებისგან შექმნილი თავისუფალი საზოგადოება, დავექვემდებარებით თუ არა სახელმწიფოსგან ტოტალურ კონტროლს ან/და დიდი კორპორაციების მანიპულაციას, შეგვეძლება თუ არა თავისუფალი არჩევნების ჩატარება და გვექნება თუ არა დემოკრატია. სწორედ აღნიშნული სიკეთეები და ღირებულებები დევს სასწორზე, რის გამოც თანამედროვე თავისუფალი სამყაროს ქვეყნები/ საზოგადოებები მზად არიან, დრო და ენერგია გაიღონ მონაცემთა დაცვაზე ზრუნვისთვის.

პერსონალურ მონაცემთა დაცვასა და ელექტრონული მმართველობის განვითარებას ხშირად წარმოაჩენენ, როგორ ურთიერთდაპირისპირებულ, კონფლიქტურ ღირებულებებს, როცა ერთის წარმატება შესაძლებელია მხოლოდ მეორის ხარჯზე, როცა ერთის აღიარება მეორის უარყოფასა და შეზღუდვას მოითხოვს. მიუხედავად იმისა, რომ ციფრული ტექნოლოგიისა და ელექტრონული მმართველობის განვითარება მართლაც მნიშვნელოვნად ზრდის და თვისობრივად განსხვავებულ სიმაღლეზე აჰყავს მონაცემთა დაცვასთან დაკავშირებული რისკები, გავრცელებულია ის აზრიც, რომ თავისთავად ტექნოლოგია არ უნდა მივიჩნიოთ პრივატულობის მტრად, რადგან თუ მონაცემთა დაცვის საკითხისადმი საკმარის ყურადღებას გამოვიჩენთ, ტექნოლოგიას შეუძლია, თავადვე ემსახუროს მონაცემთა დაცვას.

ეს ნიშნავს, რომ ციფრულ ტექნოლოგიას აქვს უნარი, თავადვე გადალახოს მისგან გამომდინარე რისკები, ამისთვის კი მისი სწორი და მიზანმიმართული გამოყენებაა საჭირო.

სხვაგვარად რომ ვთქვათ, თუ ციფრული ტექნოლოგიის/ელექტრონული მმართველობის დანერგვისას პრიორიტეტად მივიჩნევთ პერსონალურ მონაცემთა დაცვას და მასზე ისევე ვიზრუნებთ, როგორც მმართველობითი ამოცანის მიღწევაზე, ანუ თუ ისეთივე ძალისხმევას გავწევთ მონაცემთა დაცვაზე, როგორც მმართველობითი ამოცანის მიღწევაზე, ორივე საკითხში შეიძლება წარმატებას მივაღწიოთ.

დღეისათვის უკვე არსებობს გარკვეული წესების/სტანდარტების და ტექნოლოგიური გადაწყვეტილებების ერთობლიობა და შესაბამისი კარგი პრაქტიკის მაგალითები იმის თაობაზე, თუ როგორ შეიძლება პერსონალური მონაცემების დაცვასთან დაკავშირებული რისკები თავად ტექნოლოგიით შევამციროთ. ამ ტექნოლოგიებს მოიხსენიებენ შემდეგი ტერმინებით: „privacy-sensitive“, „privacy enhancing“ ან „privacy respecting“ ტექნოლოგიები.

როგორც ციფრული ტექნოლოგია არ არის თავისთავად პრივატულობის მტერი, ასევე პერსონალური მონაცემების დაცვა არ გულისხმობს მონაცემთა დამუშავების აკრძალვას. მონაცემთა დაცვის კანონმდებლობა ელექტრონული მმართველობის შეფერხებას არ განიზრახავს, როგორც ამას ჩვენს რეალობაში ხშირად არასწორად/უტრირებულად აღიქვამენ და წარმოაჩენენ. პერსონალურ მონაცემთა დაცვის შესახებ თანამედროვე კანონმდებლობა –ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაციით დაწყებული, ეროვნული კანონმდებლობებით გაგრძელებული – მიზნად ისახავს არა მონაცემთა დამუშავების აკრძალვას ან/და ელექტრონული მმართველობის შეზღუდვას, არამედ მონაცემთა დაცვის გონივრული გარანტიების შექმნას, მომხმარებელთა ნდობის უზრუნველყოფას და ამ გზით ტექნოლოგიების უსაფრთხო გამოყენების მხარდაჭერას. მონაცემთა დაცვის შესახებ თანამედროვე კანონმდებლობა – ეს არ არის აკრძალვების კანონმდებლობა, ეს კანონმდებლობაა ოპტიმალური ბალანსისა და რისკების მართვის შესახებ. შესაბამისად, ელმმართველობის ხელშემშლელ ფაქტორად მისი განხილვა უსაფუძვლოა.

ელექტრონული მმართველობის ინიციატივების წარმატებისთვის, ანუ იმისთვის, რომ მომხმარებელმა ის ეფექტიანად გამოიყენოს, მნიშვნელოვანია, მის მიმართ ნდობა არსებობდეს. საჯარო ადმინისტრაციისადმი ნდობის საკითხი ელექტრონული მმართველობის კონტექსტში სწორედ პერსონალური მონაცემების დაცვის რისკებს უკავშირდება. ეკონომიკურად განვითარებულ ქვეყნებში, რომლებშიც ინტერნეტის გამოყენების და ელსერვისების მოხმარების მაჩვენებელი შედარებით მაღალია, ელექტრონულ მმართველობასთან დაკავშირებული შფოთვა სწორედ პერსონალური მონაცემების დაცვას უკავშირდება.

რაც შეეხება საქართველოს, სამწუხაროდ ამ დროისთვის არ მოგვეპოვება სიღრმისეული/საფუძვლიანი კვლევის შედეგები იმაზე, თუ რა როლს ასრულებს მონაცემთა დაცვასთან დაკავშირებული შიში/წუხილი ელექტრონული სერვისების მოხმარებისას. შესაძლოა პერსონალურ მონაცემთა დაცვის საკითხი ქართული საზოგადოების მნიშვნელოვანი ნაწილისთვის ჯერ კიდევ სიახლეს წარმოადგენს და ელექტრონული სერვისების მოხმარების მაჩვენებელზე ჯერჯერობით მხოლოდ სხვა ფაქტორები ახდენს გავლენას (კომპიუტერის

მოხმარების უნარები, თავად ელსერვისების გამართულობა და სირთულე/სიმარტივე, ინტერნეტზე წვდომის მაჩვენებელი და ა.შ.) მაგრამ სახელმწიფო ინსპექტორის სამსახურისადმი მიმართვიანობის დინამიკას თუ შევხედავთ, აშკარაა, რომ პერსონალური მონაცემების დაცვის საკითხში საზოგადოების ინფორმირებულობის დონე იზრდება და სავარაუდოა, რომ ის გავლენას იქონიებს ელმმართველობისადმი დამოკიდებულებაზეც.

ამ თვალსაზრისით შეიძლება ითქვას, რომ პერსონალური მონაცემების დაცვა – მაღალი, ევროპული სტანდარტის კანონმდებლობის შემუშავება, მისი თანმიმდევრული დანერგვა და მონაცემთა დაცვის გარანტიების შექმნა, არათუ ხელს უშლის, არამედ ელექტრონული მმართველობის ხელშემწყობ ფაქტორად გვევლინება, რამდენადაც ის უზრუნველყოფს მომხმარებელთა ნდობას მონაცემთა დამუშავების სისტემებისადმი.

მნიშვნელოვანია, რომ ელექტრონული მმართველობის ინიციატივების/პროექტების დაგეგმვისას, დასაწყის სტადიაზევე გავითვალისწინოთ პერსონალურ მონაცემთა დაცვის საკითხი, რათა საინფორმაციო სისტემის დიზაინშივე დაიგეგმოს მონაცემთა დამუშავების პრინციპები, წინასწარვე ამოცნობილ იქნეს რისკები და დაიგეგმოს შესაბამისი გადაწყვეტები.

განვითარებულ, დემოკრატიულ სახელმწიფოებში, სადაც პერსონალურ მონაცემთა დაცვის შედარებით ხანგრძლივი ისტორია და მაღალი კულტურაა, ელექტრონული მმართველობის სისტემების შექმნისას განსაკუთრებული ყურადღებით ეკიდებიან პერსონალურ მონაცემთა დაცვის საკითხს და, შეიძლება ითქვას, რომ სისტემების შექმნის დროს, მის ეფექტურობასა და ტექნიკურ გამართულობასთან ერთად, თანაბარმნიშვნელოვან საზრუნავად მიიჩნევენ პერსონალურ მონაცემთა დაცვას. შესაბამისად, ელექტრონული სისტემის ყველა კონცეპტუალურ, სამართლებრივ-პროცედურულ და ტექნოლოგიურ საკითხს სწორედ ამ ჭრილში განიხილავენ/გადაწყვეტენ.

მონაცემთა დაცვის ძირითადი კონცეფციები, რომელთა ცოდნა მნიშვნელოვანია ელექტრონული მმართველობის დანერგვისას

მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნის პროცესში და მონაცემთა დაცვა პირველად პარამეტრად

მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნის პროცესში და მონაცემთა დაცვა პირველად პარამეტრად (Privacy by design and by default) ნიშნავს, რომ მონაცემთა დაცვის წესები ინტეგრირებული/ჩაშენებული უნდა იყოს მონაცემთა დამუშავებასთან დაკავშირებულ სისტემებში, პროცესებსა თუ პროდუქტებში მათი შექმნის მომენტიდან და შემდეგ მთელი სასიცოცხლო ციკლის განმავლობაში. ესე

იგი, მონაცემთა დაცვის პრინციპები თავიდანვე უნდა იქნეს გათვალისწინებული ყველა-ფერში, რასაც მონაცემთა დამმუშავებელი აკეთებს და რაც პერსონალურ მონაცემთა და-მუშავებას გულისხმობს. ამავე დროს, მონაცემთა დამმუშავებელს უნდა შეეძლოს აღნიშ-ნული საკითხის დემონსტრირება.

ის, რომ მონაცემთა დაცვის საკითხი შექმნის პროცესშივე უნდა იყოს გათვალისწინებული, მხოლოდ დროის მონაკვეთს არ გულისხმობს და არ ნიშნავს, თითქოს ეს მხოლოდ სისტე-მის დიზაინის საწყის ეტაპზეა გასათვალისწინებელი. „by design“ ნიშნავს, რომ მონაცემთა დაცვის პრინციპები სისტემის დიზაინშია ჩადებული – რომელიც, ერთი მხრივ, სისტემის შე-მუშავების პროცესში უნდა შეიქმნას, შემდეგ კი ეტაპობრივად გადაიხედოს.

კონცეფცია რომელიც საფუძვლად უდევს data protection by design and by default მიდგო-მას, სიახლე სულაც არაა და არც GDPR-ს შემოუტანია, არამედ ის მანამდეც არსებობდა „privacy by design“ სახელით და ამერიკის შეერთებულ შტატებში უკვე 90-იანი წლებიდან გამოიყენებოდა.

თუმცა ბოლო წლების სიახლე ისაა, რომ ევროკავშირის მონაცემთა დაცვის ზოგადმა რე-გულაციამ (GDPR), რომელიც 2018 წლის მაისში ამოქმედდა, ის შესასრულებლად სავალდე-ბულო გახადა ევროკავშირის ტერიტორიაზე მონაცემთა დამუშავების შემთხვევებისთვის.

„Data protection by design and by default“ მიდგომა არ გულისხმობს მონაცემთა დაცვის ახალი, დამატებითი პრინციპების დადგენას (მაგალითად, ისეთების, როგორებიცაა მიზნის შეზღუდვა, დამუშავების მინიმიზაცია და ა.შ.), არამედ ეს არის მიდგომა, თუ როგორ და რა გზით უნდა უზრუნველყოს მონაცემთა დამმუშავებელმა უკვე არსებული პრინციპების დაც-ვა/დანერგვა. ე.ი. მონაცემთა დამმუშავებელმა სისტემის დაგეგმვის საწყის ეტაპზევე უნდა დაიწყოს ზრუნვა მონაცემთა დაცვაზე – სისტემაში ჩააშენოს ისეთი ტექნიკური და ორგანი-ზაციული ზომები, რომლებიც უზრუნველყოს მონაცემთა დაცვის პრინციპების რეალიზებას.

„Data protection by design and by default“ მიდგომა ნიშნავს, რომ მონაცემთა დამმუშავე-ბელმა მთლიანი ორგანიზაციის მასშტაბით, მის ყველა ასპექტში უნდა დანერგოს საკუთარი მიდგომა მონაცემთა დაცვის საკითხისადმი და ჩააშენოს მონაცემთა დაცვის პრინციპები მონაცემთა დამუშავების ყველა აქტივობაში, რომელსაც აწარმოებს. ამასთან, როდესაც მონაცემთა დამმუშავებელი განიხილავს ელექტრონული მმართველობისთვის საჭირო სერვისების/პროდუქტების შეძენას სხვა მომწოდებლებისგან, უნდა ეძებოს და შეარჩიოს შესაბამისი დეველოპერები/დიზაინერები, რომლებიც თავიანთი პროდუქტების განვითა-რებისას ყურადღებას აქცევენ მონაცემთა დაცვის საკითხებს.

უფრო კონკრეტულად, „Privacy by design“ გულისხმობს, რომ მონაცემთა დამმუშავებელ-მა სისტემის შექმნის საწყის ეტაპზე, ანუ მონაცემთა დამუშავების საშუალებების განსაზღვ-რისას და შემდეგ უკვე დამუშავების პროცესში მუდმივად უნდა უზრუნველყოს სათანადო ტექნიკური და ორგანიზაციული ზომების არსებობა, რაც, თავის მხრივ, უზრუნველყოფს,

რომ პრაქტიკაში ეფექტურად იყოს დაცული/რეალიზებული მონაცემთა დამუშავების პრინციპები; ასევე უნდა მოახდინოს ისეთი ზომების ინტეგრირება, რითაც დაცული იქნება მონაცემთა სუბიექტის უფლებები.

Data protection by default გულისხმობს, რომ მონაცემთა დამმუშავებელმა უნდა დანერგოს სათანადო ტექნიკური და ორგანიზაციული ზომები, რათა, როგორც საწყისი პარამეტრი (by default), მუშავდებოდეს მხოლოდ პერსონალური მონაცემების ის მინიმუმი, რაც აუცილებელია დამუშავების კონკრეტული მიზნის მისაღწევად. ამ თვალსაზრისით დამუშავების მინიმიზაცია ეხება როგორც შეგროვებულ მონაცემთა ოდენობას/კატეგორიებს, ისე დამუშავების ფარგლებს, შენახვის ვადას და მათზე ხელმისაწვდომობას. „By default" მონაცემები ხელმისაწვდომი არ უნდა იყოს პირთა განუსაზღვრელი წრისთვის, მონაცემთა სუბიექტის ჩარევის/ნების გამოხატვის გარეშე.

Data protection by default გულისხმობს, რომ პერსონალური მონაცემები უნდა იყოს ავტომატურად დაცული ნებისმიერ საინფორმაციო სისტემაში, სერვისში, პროდუქტში, ისე რომ მონაცემთა სუბიექტს არ უნდა სჭირდებოდეს რაიმე კონკრეტული ქმედების განხორციელება მისი მონაცემების დაცვისთვის.

Privacy by default – გულისხმობს, რომ რეალიზებული იქნება „პრივატულობა უპირველეს ყოვლისა" (privacy-first) მიდგომა, როგორც პირველადი (default) პარამეტრი სისტემაში; ამავე დროს, მნიშვნელოვანია, რომ დამმუშავებელმა არ შესთავაზოს მონაცემთა სუბიექტს ილუზორული არჩევანი იმასთან დაკავშირებით, თუ რა მონაცემი მუშავდება სისტემაში მის შესახებ, ანუ გასაგები ენით უნდა აუხსნას რა მონაცემების დამუშავებას მოითხოვს/გულისხმობს სისტემა უპირობოდ, რასთან მიმართებითაც სუბიექტს არჩევანი არ აქვს, ხოლო სხვა ყოველგვარი დამატებითი დამუშავება დამოკიდებული უნდა იყოს მონაცემთა სუბიექტის გადაწყვეტილებაზე,– ანუ მისი რეალური არჩევანი უნდა იყოს.

აღნიშნული კონცეფციის მიდგომა – რომ მონაცემთა დაცვის პრინციპები გათვალისწინებული და ინტეგრირებული იყოს სისტემის დიზაინში, ნიშნავს იმას, რომ მონაცემთა დამუშავების სისტემის ტექნიკური, ინფრასტრუქტურული თუ ორგანიზაციული გადაწყვეტები პასუხობდეს მონაცემთა დაცვის საჭიროებებს, მონაცემთა დაცვის კანონმდებლობით დადგენილ პრინციპებს და ქმნიდეს მათი აღსრულების შესაძლებლობას. მაგალითად, თუ ორგანიზაციის მონაცემთა დამუშავების სისტემაში რამდენიმე ასეული, სრულიად განსხვავებული როლებისა და ფუნქციების მქონე თანამშრომელია ჩართული, „მონაცემთა მინიმიზაციის" პრინციპი მოითხოვს, რომ აღნიშნული სისტემის მომხმარებლებს მხოლოდ მათი როლებიდან და საჭიროებებიდან გამომდინარე ინფორმაციაზე ჰქონდეთ დაშვება და მხოლოდ – დროის საჭირო მონაკვეთში. ეს კი ნიშნავს, რომ მონაცემთა დამუშავების სისტემას უნდა შეეძლოს მრავალი კატეგორიის მომხმარებლის შექმნა და მათი სპეციფიკური როლებით/უფლებებით აღჭურვა. by design-ის ამოცანაა, რომ სისტემის აღნიშნული თავისებურება და მონაცემთა დაცვის კანონმდებლობიდან მომდინარე საჭიროებები გათ-

ვალისწინებული იქნეს ამ სისტემის დიზაინისას და ტექნიკურად შესაძლებელი იყოს მონაცემთა მინიმიზაციის პრინციპის დაცვა.

ასევე მაგალითად, მონაცემთა სუბიექტისთვის კანონით გარანტირებული უფლებების რეალიზება მოითხოვს, რომ ორგანიზაციას შეეძლოს ამ პირის შესახებ მასთან არსებული/დამუშავებული მონაცემების იდენტიფიცირება, ასევე ამ მონაცემების მესამე პირებისთვის გადაცემის ფაქტების იდენტიფიცირება და მონაცემთა სუბიექტისთვის შესაბამისი ინფორმაციის მიწოდება. იმისათვის, რომ პრაქტიკაში ამ მოთხოვნის შესრულება შესაძლებელი გახდეს, საჭიროა, მონაცემთა დამუშავების სისტემა თავიდანვე იმგვარად იყოს ორგანიზებული (ანუ დიზაინში იყოს გათვალისწინებული), რომ მონაცემთა ყველა სუბიექტის შესახებ არსებული ინფორმაციისა და მათზე შესრულებული ყველა მოქმედების იდენტიფიცირება/მიკვლევა შეგვეძლოს.

აქვე უნდა აღინიშნოს, რომ Data Protection by design and by default მიდგომა შეეხება არა მხოლოდ მონაცემთა ელექტრონული/ავტომატური დამუშავების სისტემებს, ელექტრონულ სერვისებსა და პროდუქტებს, არამედ ის რელევანტურია პერსონალურ მონაცემთა დამუშავებაზე/დაცვაზე გავლენის მომხდენი ნებისმიერი სისტემის მიმართ. ამ თვალსაზრისით, მისი გათვალისწინება შეიძლება საჭირო იყოს ფიზიკური ინფრასტრუქტურის დიზაინის პროცესშიც, მაგალითად, სამედიცინო მომსახურების გამწევი დაწესებულების შენობა-ნაგებობების დიზაინისას და მისი შიდა ორგანიზაციული პროცედურების შემუშავებისას.

Data protection by design and by default – მიდგომის რეალიზაციისათვის არ არსებობს რაიმე მზა რეცეპტი და წინასწარ განსაზღვრული წყება ორგანიზაციულ-ტექნიკური ზომებისა, რომელიც ყველა სისტემას მოერგება, ანუ აქ „one size fits all“ მიდგომა შეუძლებელია და გასატარებელი ზომები დამოკიდებულია კონკრეტულ გარემოებებსა და კონტექსტზე.

Data protection by design and by default მიდგომის რეალიზაციისკენ მიმართული ზომების/გადაწყვეტების მაგალითები შეიძლება იყოს:

- მონაცემთა დროული ფსევდონიმიზაცია, სადაც ეს შესაძლებელია;
- მონაცემთა დამუშავების მინიმიზაცია – საჭირო/აუცილებელი მონაცემების ზუსტი იდენტიფიცირება და მონაცემთა მინიმალური კატეგორიის შეგროვება/დამუშავება;
- თანამშრომელთა როლების/ამოცანების ანალიზი და მათი დაშვება მხოლოდ მონაცემთა საჭირო მინიმუმზე, მინიმალური დროით;
- გარკვეული მომენტის დადგომისას (როცა მიზანი მიღწეულია) დამუშავების ავტომატური შეწყვეტა ან/და მათზე წვდომის შეზღუდვა;
- მაქსიმალური გამჭვირვალობა სისტემის ფუნქციონირებასთან დაკავშირებით და სუბიექტისთვის შესაძლებლობის მიცემა, აკონტროლოს/მონიტორინგი გაუწიოს დამუშავების პროცესს;
- მონაცემთა დამმუშავებელმა მონაცემთა დაცვის საკითხი თავისი ნებისმიერი სისტემისა თუ პროდუქტის დიზაინისა და იმპლემენტაციის განუყოფელ ნაწილად უნდა აქციოს.

მონაცემთა დაცვა უნდა განიხილებოდეს, როგორც მონაცემთა დამუშავების სისტემის ძირითადი ფუნქციონალის არსებითი კომპონენტი.

Privacy by design and by default დაკავშირებულია მონაცემთა დაცვაზე გავლენის შეფასების (DPIA) საკითხთან, რომელსაც შემდეგ ქვეთავში/ნაწილში განვიხილავთ.

მონაცემთა დაცვაზე გავლენის შეფასება (DPIA)

მონაცემთა დაცვაზე გავლენის შეფასება (DPIA) არის ინსტრუმენტი, რომელიც ეხმარება მონაცემთა დამმუშავებელს, ამოიცნოს ამა თუ იმ პროექტის/საინფორმაციო სისტემის პერსონალურ მონაცემთა დაცვასთან დაკავშირებული რისკები და მოახდინოს რაც შეიძლება შეამციროს ისინი. სხვაგვარად რომ ითქვას, DPIA საშუალებაა, რომ მონაცემთა დამმუშავებელმა სისტემატურად და საფუძვლიანად გააანალიზოს თავისი მონაცემთა დამუშავების სისტემები, ამოიცნოს და შეამციროს მონაცემთა დაცვასთან დაკავშირებული რისკები. ის ასევე ხელს უწყობს მონაცემთა დამმუშავებლებს, უფრო ეფექტიანად წარმართონ მონაცემთა დამუშავების სისტემების დიზაინი.

რამდენადაც Data protection by design and by default გულისხმობს რისკების პროპორციული, ორგანიზაციული და ტექნიკური ზომების გატარებას მონაცემთა დაცვის პრინციპების შესასრულებლად, DPIA სწორედ რისკების ანალიზის საფუძველზე ეხმარება დამმუშავებელს, სწორად განსაზღვროს მის მიერ გასატარებელი ორგანიზაციული და ტექნიკური ზომები.

რისკების დონის შეფასებისას დამმუშავებელმა, ცხადია, უნდა გაითვალისწინოს როგორც რისკის რეალიზების ალბათობა, ისე მონაცემთა დამმუშავებელზე შესაძლო გავლენის სიმძიმე. რასაკვირველია, DPIA-ს ჩატარება არ ნიშნავს რისკების სრულად განეიტრალებას, შეიძლება გარკვეული რისკები დარჩეს, თუმცა DPIA დამმუშავებელს ეხმარება, მოახდინოს მათი დოკუმენტირება და შეაფასოს, არის თუ არა დარჩენილი რისკები დასაბუთებული.

DPIA-ის პროცესის ჩატარება, ზოგადად, კარგ პრაქტიკად ითვლება ნებისმიერ მონაცემთა დამუშავების სისტემასთან მიმართებით, თუმცა მისი ჩატარება რეკომენდებულია (ზოგ შემთხვევაში/ქვეყნებში კი – სავალდებულო) მონაცემთა დამუშავების ისეთი სისტემებისთვის, რომლებსაც მონაცემთა დაცვის თვალსაზრისით მაღალი რისკები უკავშირდება. მაგალითად, ასეთად მიჩნეულია, შემთხვევები, როდესაც წარმოებს/იგეგმება:

- განსაკუთრებული კატეგორიის მონაცემების დამუშავება;
- საჯარო სივრცეების სისტემატური მონიტორინგი;
- მონაცემთა სუბიექტის პროფილირების გამოყენება და ავტომატური გადაწყვეტილებების მიღება (automated decision-making);
- მონაცემთა სუბიექტების ფართომასშტაბიანი პროფილირება;
- ბიომეტრიული ან გენეტიკური მონაცემების დამუშავება.

ბავშვთა პერსონალური მონაცემების დამუშავება პროფილირებისთვის ან ავტომატური გადაწყვეტილებისთვის, ან მარკეტინგული მიზნებისთვის, ან/და ონლაინ სერვისების შეთავაზებისთვის და სხვა.

DPIA უნდა ჩატარდეს მონაცემთა დამუშავების პროცესის დაწყებამდე, მონაცემთა დამუშავების სისტემის დიზაინის ფაზაში, თუ შესაძლოა, რომ მონაცემთა დამუშავებას თან ახლდეს მაღალი რისკები. მართალია, ამ ეტაპზე რისკების დონე კონკრეტულად შეფასებული არ არის, მაგრამ ხდება იმ ფაქტორების იდენტიფიცირება, რომლებიც მიანიშნებენ მონაცემთა სუბიექტის მიმართ შესაძლო უარყოფითი გავლენების პოტენციალზე, და ამის მიხედვით მიიღება გადაწყვეტილება მონაცემთა დაცვაზე გავლენის შეფასების თაობაზე.

DPIA პროცესი გულისხმობს რომ, უნდა:

- აღიწეროს პერსონალურ მონაცემთა დამუშავების ბუნება/სახე, ფარგლები, კონტექსტი და დამუშავების მიზნები;
- გაანალიზდეს და შემოწმდეს, არის თუ არა მონაცემთა დაგეგმილი დამუშავება აუცილებელი და მიზნის პროპორციული და აღიწეროს, როგორ იქნება უზრუნველყოფილი შესაბამისობა მონაცემთა დაცვის პრინციპებთან;
- მოხდეს რისკების იდენტიფიცირება, გაანალიზდეს მათი რეალიზების ალბათობა და სიმძიმე მონაცემთა სუბიექტების უფლებებისა და ინტერესებისადმი;
- განისაზღვროს ორგანიზაციულ-ტექნიკური ზომები, რომლებიც უნდა გატარდეს რისკების აღმოსაფხვრელად ან შესამცირებლად.
- მოხდეს DPIA-ის პროცესისა და ამ პროცესში მიღებული გადაწყვეტილებების დოკუმენტირება, მათ შორის ამ პროცესში განხილული ყოველი განსხვავებული აზრის/ალტერნატივის;
- რისკებთან გასამკლავებლად იდენტიფიცირებული ზომების ინტეგრირება უნდა მოხდეს შესაბამისი პროექტის სამოქმედო გეგმაში.

DPIA-ს პერიოდულად უნდა გადახედონ და განიხილონ

მნიშვნელოვანია, მონაცემთა დამმუშავებელმა მოახდინოს DPIA-ის, როგორც ორგანიზაციული პროცესის ინტეგრირება/დანერგვა და უზრუნველყოს, რომ DPIA შედეგები რეალურად გავლენას ახდენდეს მის გადაწყვეტილებებზე.

მიზნის შეზღუდვის პრინციპი

პერსონალურ მონაცემთა დაცვის სფეროში ერთ-ერთი საკვანძო ამოცანაა მონაცემთა დამუშავების მიზნის განსაზღვრა და მასთან დაკავშირებული საკითხების რეგლამენტაცია.

როგორც საერთაშორისო სამართლებრივი აქტები, ისე ქართული, ევროპული და სხვა მრავალი ქვეყნის კანონმდებლობა ადგენს პრინციპს, რომელსაც ინგლისურენოვან ლიტერატურაში „მიზნის შეზღუდვის“ (purpose limitation) პრინციპად მოიხსენიებენ და რომელიც მონაცემთა დაცვის კანონმდებლობის ქვაკუთხედია.

ქართულ კანონმდებლობაში აღნიშნული პრინციპი შემდეგნაირადაა ფორმულირებული: „მონაცემები შეიძლება დამუშავდეს მხოლოდ კონკრეტული, მკაფიოდ განსაზღვრული, კანონიერი მიზნებისათვის. დაუშვებელია მონაცემთა შემდგომი დამუშავება სხვა, თავდაპირველთან შეუთავსებელი მიზნით“.

აღნიშნული პრინციპი, მრავალი თვალსაზრისით, უაღრესად აქტუალურია ელექტრონული მმართველობის კონტექსტში, განსაკუთრებით კი ელექტრონული მმართველობისთვის სასიცოცხლოდ მნიშვნელოვან ისეთ პრინციპებთან კვეთის გამო, როგორებიცაა „Once Only“ და „მონაცემთა ხელახალი გამოყენება“. გარდა ამისა, ქართულ რეალობაში მონაცემთა დაცვის საკითხის შედარებით ნაკლები ცნობილობის გამო ხშირია ცდუნება იმისა, რომ ერთი კონკრეტული მიზნით შეგროვებული პერსონალური მონაცემები სხვა, არცთუ თავსებადი მიზნის მისაღწევად იქნეს გამოყენებული.

„მიზნის შეზღუდვის“ პრინციპის არსი ისაა, რომ მონაცემები არ შეიძლება შეგროვდეს ან სხვაგვარად დამუშავდეს ზოგადი, აბსტრაქტული და ბუნდოვანი მიზნით. დამუშავების ნამდვილი მიზანი კონკრეტულად, ერთმნიშვნელოვნად და ასევე მონაცემთა სუბიექტისთვის გასაგები ფორმით (გასაგებ ენაზე) უნდა იყოს ჩამოყალიბებული.

ნებისმიერი ელექტრონული სისტემის შექმნამდე და პერსონალურ მონაცემთა დამუშავების დაწყებამდე მისი მიზნის სწორად გააზრება და დაკონკრეტება აუცილებელი წინაპირობაა მონაცემთა შემდგომი დამუშავების კანონიერებისთვის. სწორედ მონაცემთა დამუშავების მიზნიდან გამომდინარე უნდა განისაზღვროს დასამუშავებელი მონაცემების კატეგორია, მოცულობა, დამუშავების/შენახვის ვადა და სხვა არსებითი ასპექტები.

უპირველეს ყოვლისა, მნიშვნელოვანია, დამუშავების მიზანი იმდენად კონკრეტული იყოს, რომ შესაძლებლობას იძლეოდეს, ამ მიზნიდან გამომდინარე მოხდეს მონაცემთა დამუშავების საჭირო ფარგლების დადგენა.

მონაცემთა დამუშავების მიზნის დაკონკრეტება და მისი მკაფიოდ ფორმულირება ხელს უწყობს ამ პროცესის გამჭვირვალობასა და ლოგიკურობას, რაც ასევე აუცილებელი პირობაა მონაცემთა დამუშავების ლეგიტიმაციისათვის. მისი საშუალებით წინასწარ ცნობილი ხდება საზღვრები, რომელთა ფარგლებშიც დამმუშავებელს შეუძლია პროცესის შესრულება და ეს ხელს უწყობს მონაცემთა შემდგომი გამოყენების თაობაზე მხარეთა ერთგვაროვან მოლოდინებს, შესაბამისად, ამცირებს რისკებს, რომ მონაცემთა სუბიექტსა და დამმუშავებელს განსხვავებული მოლოდინები/წარმოდგენები ჰქონდეთ მონაცემთა დამუშავების მასშტაბებსა და მოცულობაზე.

ამავე დროს, მონაცემთა დამუშავების მიზანი უნდა იყოს კანონიერი. აქ იგულისხმება კანონიერება ფართო გაგებით და არა მხოლოდ პერსონალურ მონაცემთა დაცვის შესახებ კანონთან შესაბამისობა. ე.ი. გასათვალისწინებელია მთლიანად ქვეყანაში მოქმედი სამართლებრივი წესრიგი, გარდა იმისა, რომ უნდა გვქონდეს მონაცემთა დამუშავების შესახებ კანონით განსაზღვრული საფუძველი. დამუშავება კანონიერი უნდა იყოს, მაგალითად, იმ თვალსაზრისითაც, რომ მონაცემთა დამუშავების პირდაპირი ან ირიბი შედეგი არ გახდეს დისკრიმინაციული გადაწყვეტილებები მონაცემთა სუბიექტების თუ სხვა პირების მიმართ.

როდის უნდა განისაზღვროს მონაცემთა დამუშავების მიზანი?

მონაცემთა დამუშავების მიზნის განსაზღვრა ერთ-ერთი პირველია, რაც მონაცემთა დამმუშავებელმა უნდა მოიმოქმედოს დამუშავების სისტემის, პროექტისა თუ სერვისის დაგეგმვისას ანუ მონაცემთა დამუშავების დაწყებამდე. სწორედ ამის გათვალისწინებით უნდა მიიღონ შემდგომი გადაწყვეტილებები დამუშავების მოცულობის, ფარგლების, ვადებისა და ა.შ. შესახებ. მონაცემთა დამმუშავებელმა არა მხოლოდ უნდა განსაზღვროს მიზნები, არამედ უნდა მოახდინოს მისი დოკუმენტირება და, საჭიროების შემთხვევაში, შეძლოს ამის დემონსტრირება.

საქართველოს მოქმედი კანონმდებლობა პირდაპირ არ ადგენს მონაცემთა დამუშავების მიზნის განსაზღვრის მომენტს და ფორმას, თუმცა ამ პრინციპის არსიდან გამომდინარე, შეიძლება ერთმნიშვნელოვნად ითქვას, რომ მიზანი უნდა განისაზღვროს წინასწარ, მონაცემების დამუშავებამდე (შეგროვებამდე) ან არაუგვიანეს შეგროვების პროცესში.

როგორც ზემოთ აღვნიშნეთ, მიზანი „მკაფიოდ განსაზღვრული“, შესაბამისად, კონკრეტული, არაორაზროვანი და მონაცემთა სუბიექტისთვის შეძლებისდაგვარად ადვილად გასაგები უნდა იყოს.

მონაცემთა დამუშავების მიზნის კონკრეტულობა გულისხმობს, რომ მონაცემთა დამუშავების ფარგლების, მოცულობისა და ვადების შეფასება შესაძლებელი იყოს ამ მიზნებთან მიმართებით.

ამიტომ მონაცემთა დამუშავების ზოგადი მიზანი, მაგალითად, როგორებიცაა: „მომსახურების ხარისხის გაუმჯობესება“, „მარკეტინგული მიზნები“, „IT უსაფრთხოება“ და ა.შ. შემდგომი დეტალიზების გარეშე ყოველთვის არ აკმაყოფილებს „მკაფიოდ განსაზღვრული“ მიზნის პრინციპს. დეტალიზების ხარისხი, რა თქმა უნდა, დამოკიდებულია კონტექსტზე, რომელშიც მონაცემები გროვდება, და თავად მონაცემების შინაარსზე.

მიზნის მკაფიოდ განსაზღვრა არ ნიშნავს, რომ მიზნის ვრცელი და დეტალური აღწერა თავისთავად კარგი და სასარგებლოა – ეს შეიძლება საწინააღმდეგო შედეგის მომტანიც კი იყოს. შესაძლოა გვქონდეს შემთხვევა, როდესაც მიზნის ვრცელი, ერთი შეხედვით დეტალური და სამართლებრივად გამართული წერილობითი ფორმულირება სინამდვილეში

პასუხისმგებლობის თავიდან არიდებას ემსახურებოდეს და სულაც არ შეიცავდეს სასარგებლო ინფორმაციას მონაცემთა სუბიექტისა თუ სხვა დაინტერესებული მხარეებისათვის.

პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონი ადგენს, რომ ***„დაუშვებელია მონაცემთა შემდგომი დამუშავება სხვა, თავდაპირველ მიზანთან შეუთავსებელი მიზნით“.*** ეს ნიშნავს, რომ ერთი კონკრეტული მიზნით დამუშავებული/შეგროვებული პერსონალური მონაცემები ამ მიზნის მიღწევის შემდეგ, როგორც წესი, აღარ უნდა გამოიყენონ სხვა მიზნით, გარდა იმ შემთხვევებისა, როდესაც ახალი მიზანი შეთავსებადია თავდაპირველ მიზანთან. შეთავსებადობის პრობლემა საერთოდ არ წარმოიშობა, როდესაც მონაცემთა შემდგომი გამოყენება ხდება საარქივო, კვლევითი ან/და სტატისტიკური მიზნებით.

მონაცემთა შეგროვების თავდაპირველ მიზანსა და მისი შემდგომი დამუშავების შეთავსებადობის შესაფასებლად საერთაშორისო პრაქტიკაში გამოიყენება რამდენიმე კრიტერიუმი, რომლებიც ამ პროცესში გასათვალისწინებელია.

მონაცემთა შეგროვების თავდაპირველი და შემდგომი მიზნების ურთიერთკავშირი

თავსებადობის საკითხის შესაფასებლად უპირველესად უნდა დადგინდეს, რა კავშირი და ურთიერთმიმართებაა თავდაპირველ მიზანსა და დამუშავების შესაძლო შემდგომ მიზანს შორის. აქ ყურადღება უნდა გამახვილდეს არა მხოლოდ ტექსტობრივ შესაბამისობაზე, არამედ ურთიერთობის არსზე. შესაძლოა, ტექსტიდან პირდაპირ არ იკითხებოდეს მიზნებს შორის შესაბამისობა, ტექსტები არ ემთხვეოდეს ერთმანეთს, მაგრამ არსობრივად უკავშირდებოდეს.

ზოგჯერ საქმე მარტივადაა – თავდაპირველ მიზანში შეიძლება პირდაპირ იგულისხმებოდეს შემდგომი მიზანი, ან მონაცემთა შემდგომი გამოყენება პირდაპირ გამომდინარეობდეს მიზნიდან, ზოგჯერ კი საერთოდ მიზნებს შორის კავშირი ცხადად არ ჩანს და მთლიანი კონტექსტის განხილვაა საჭირო. მნიშვნელოვანია, გავითვალისწინოთ მიღებული ფაქტობრივი კონტექსტი და ის, თუ კონკრეტული მიზანი (თავდაპირველად რაც დასახელდა), როგორც წესი, როგორ გაიგება შესაბამისი მხარეების მიერ მსგავს სიტუაციებში.

ასევე უნდა გავითვალისწინოთ მონაცემთა შეგროვების კონტექსტი და მისგან გამომდინარე მონაცემთა სუბიექტის გონივრული მოლოდინი მონაცემთა შემდგომ გამოყენებაზე. ანუ უნდა ვივარაუდოთ, რა მოლოდინი შეიძლება გაუჩნდეს ლოგიკურად მონაცემთა სუბიექტს, მისი ინფორმაციის შეგროვების კონტექსტიდან გამომდინარე.

ამ თვალსაზრისით, მნიშვნელოვანი ასპექტია მონაცემთა დამმუშავებლისა და მონაცემთა სუბიექტის ურთიერთობის თავისებურება და ბუნება. აქ იგულისხმება არა მხოლოდ სამართლებრივი მხარე და განაცხადი მონაცემთა შეგროვების მიზანზე, არამედ სამომხმარებ-

ლო და ზოგადი ლოგიკიდან გამომდინარე მოლოდინები მოცემულ კონტექსტში, მოცემულ ადმინისტრაციულ-სამართლებრივ ურთიერთობებში. ამ თემაზე ისიც უნდა აღინიშნოს, რომ ზოგჯერ კონტექსტი შეიძლება საერთოდ გამორიცხავდეს მონაცემთა შემდგომ – სხვა მიზნით გამოყენებას.

მონაცემთა ბუნება და დამუშავების შესაძლო გავლენა/შედეგები

მონაცემთა შემდგომი გამოყენების თავსებადობის შეფასებისას განსაკუთრებული ყურადღება უნდა დაეთმოს თავად ინფორმაციის შინაარსს და შემდგომი გამოყენების შედეგებს მონაცემთა სუბიექტისათვის. ზოგადად დამუშავების პროცესში მყოფი ინფორმაციის შინაარსს, მის კატეგორიას (სენსიტიურობას)არსებითი მნიშვნელობა აქვს მონაცემთა დაცვის კანონმდებლობით დადგენილი სხვადასხვა პრინციპების განმარტებისა და კონტექსტის შეფასების დროს.

ამიტომ მნიშვნელოვანია შევაფასოთ, მონაცემთა შემდგომი გამოყენება რამდენად გულისხმობს „სენსიტიური“ მონაცემების გამოყენებას ან ისეთი მნიშვნელოვანი ინფორმაციის დამუშავებას, როგორიცაა ფინანსებთან ან კომუნიკაციებთან დაკავშირებული ინფორმაცია, ადგილმდებარეობასთან დაკავშირებული ინფორმაცია და სხვა. ე.ი., რაც მეტად „სენსიტიურ“ ინფორმაციასთან გვაქვს საქმე, მით მეტად კრიტიკული უნდა იყოს საინფორმაციო სისტემის მფლობელი და მით უფრო მკაცრად უნდა შეხედოს თავსებადობის საკითხს.

როდესაც მონაცემთა შემდგომი დამუშავების შედეგებზე ვსაუბრობთ, მათი შეფასებისას უნდა გავითვალისწინოთ მონაცემთა დამუშავების გზებიც – მაგალითად, მონაცემების შემდგომი დამუშავება ხომ არ გულისხმობს სხვა დამმუშავებლის ხელში მის მოხვედრას სუბიექტისთვის უცნობი შედეგებით, მონაცემები ხომ არ ხდება საჯაროდ ან ადამიანთა ფართო წრისთვის ხელმისაწვდომი.

რაც მეტად ნეგატიური და უჩვეულო/არაპროგნოზირებადი შედეგი შეიძლება მოჰყვეს ინფორმაციის შემდგომ დამუშავებას, მით ნაკლებად თავსებადად შეიძლება მივიჩნიოთ პირველად მიზანთან.

ასევე უნდა გავითვალისწინოთ, რომ მონაცემთა დამმუშავებელს ხელი მიუწვდებოდეს სხვა ალტერნატიულ, სუბიექტისთვის უსაფრთხო მეთოდებზეც, ანუ ხელმისაწვდომია თუ არა ალტერნატიული მეთოდი იმისათვის, რომ მონაცემთა კონკრეტული გზით დამუშავების გარეშე მიაღწიოს სასურველ, კანონიერ შედეგს.

მონაცემთა დაცვის ღონისძიებები

კიდევ ერთი ფაქტორი, რომელიც მონაცემების შემდგომი დამუშავების თავსებადობის შეფასებისას უნდა გავითვალისწინოთ, პერსონალურ მონაცემთა დაცვის ღონისძიებებია – ზომები და ძალისხმევა, რასაც მონაცემთა დამმუშავებელი მიმართავს, რათა უზრუნველ-

ყოს ამ საქმიანობის კანონიერება და მონაცემთა სუბიექტზე უარყოფითი გავლენის პრევენცია.

აქვე უნდა აღინიშნოს, რომ ამგვარი მრავალფაქტორიანი შეფასებისას ეს უკანასკნელი (გატარებული ორგანიზაციულ-ტექნიკური ზომები) შეიძლება ისეთ მნიშვნელოვან ფაქტორად მივიჩნიოთ, რომლის სიმყარე აბალანსებს და გადაწონოს სხვა ფაქტორების მხრივ არსებულ სისუსტეებს და დასაშვებს ხდის მონაცემთა შემდგომ დამუშავებას. მაგალითად, ისეთი ორგანიზაციული ან ტექნიკური ზომების მიღება, როგორებიცაა მონაცემთა ნაწილობრივი ან სრული ანონიმიზაცია, ფსევდონიმიზაცია, დამატებითი ზომები გამჭვირვალობის გასაზრდელად, მონაცემთა სუბიექტისთვის დამატებითი შესაძლებლობის მიცემა, რომ აკონტროლოს ან/და საჭიროების შემთხვევაში გააპროტესტოს მონაცემთა დამუშავება, ან/და დამატებით თანხმობა გამოხატოს დამუშავებაზე. თუ მონაცემთა დამუშავების მიზანი იცვლება ან ის ნათლად და კონკრეტულად არ ყოფილა განსაზღვრული, თავსებადობის უზრუნველსაყოფად, უპირველეს ყოვლისა, საჭიროა მიზნის თავიდან სპეციფიკაცია ანუ დაკონკრეტება. ამ დროს აუცილებელია, სუბიექტს დამატებითი ინფორმაცია მიეწოდოს და კონკრეტული სიტუაციიდან და გარემოებებიდან გამომდინარე, შეიძლება საჭირო გახდეს დამატებითი საშუალების მიცემა –დაეთანხმოს ან უარყოს მისი მონაცემების დამუშავება ახლად განსაზღვრული/დაკონკრეტებული მიზნით.

მიზნის შეთავსებადობის შეფასება ყოველთვის ერთდროულად რამდენიმე კრიტერიუმს უნდა ეფუძნებოდეს. არის შემთხვევები, რომელთაც ზემოთ განხილული ვერცერთი ფაქტორი/საკითხი ვერ პასუხობს, შესაბამისად, შეფასება კონტექსტიდან გამომდინარე რელევანტური ფაქტორების ერთდროულად შესწავლას მოითხოვს.

მონაცემთა მინიმიზაცია

„მონაცემები შეიძლება დამუშავდეს მხოლოდ იმ მოცულობით, რომელიც აუცილებელია შესაბამისი კანონიერი მიზნის მისაღწევად. მონაცემები უნდა იყოს იმ მიზნის ადეკვატური და პროპორციული, რომლის მისაღწევადაც მუშავდება ისინი“.

ეს პრინციპი ყველაზე ნათლად წარმოაჩენს პერსონალური მონაცემების დაცვის კონცეფციას, რომლის არსიც არა მონაცემთა დამუშავების აკრძალვა, არამედ მისი მინიმიზაცია და პროპორციულობაა. ამ პრინციპის დაცვისთვის აუცილებელია, მონაცემთა დამმუშავებელმა, მას შემდეგ, რაც განისაზღვრება კონკრეტული მიზანი, დაადგინოს მონაცემთა ის მინიმალური მოცულობა, რომელიც აღნიშნული მიზნის მისაღწევადაა აუცილებელი და მხოლოდ ამგვარი მონაცემები დაამუშაოს. მიზნის მისაღწევად აუცილებელ მონაცემებად მიიჩნევა ის მონაცემები, რომელთა დამუშავების გარეშეც შეუძლებელია კონკრეტული, მკაფიოდ განსაზღვრული მიზნის მიღწევა. თუმცა როდესაც განიხილავთ მონაცემთა „აუცილებლობას“ და მის გარეშე მიზნის მიღწევის „შეუძლებლობას“, ჩნდება კითხვა, რამდენად

უნდა ვიგულისხმოთ მათში აბსოლუტური აუცილებლობა და შეუძლებლობა, ანუ ნიშნავს თუ არა მიზნის მიღწევის შეუძლებლობა ასეთი მიზნის მიღწევის თეორიულ გამორიცხვას? პრაქტიკაში შეიძლება წარმოიშვას სიტუაცია, როდესაც კონკრეტული, კანონიერი მიზნის მიღწევა მონაცემთა დამმუშავებელს თეორიულად კი შეუძლია, პერსონალურ მონაცემთა ერთობლიობიდან გარკვეული მონაცემების გამოკლების პირობებშიც, მაგრამ საამისოდ მას არაადეკვატური, არაპროპორციული ძალისხმევის/რესურსების გაღება მოუწევს, რაც პრაქტიკული თვალსაზრისით გამორიცხავს ან აზრს უკარგავს მის მიერ მიზნის მიღწევას და, ამავე დროს, საქმე გვაქვს ისეთ მონაცემთა დამუშავებასთან, რომელსაც დიდი ზიანი და რისკი არ მოაქვს მონაცემთა სუბიექტისთვის. ამის გათვალისწინებით, არც სიტყვა „აუცილებელია“ არ უნდა განვმარტოთ ფორმალურად და მასში არ უნდა ვიგულისხმოთ აბსოლუტური აუცილებლობა. მეორე მხრივ, ამგვარმა მიდგომამ არ უნდა მიგვიყვანოს სხვა უკიდურესობამდე – მონაცემთა დამმუშავებლებმა არ შეიძლება, უბრალოდ საქმის გამარტივებისა და გაიაფების მიზნით „აუცილებლად“ მიიჩნიონ ისეთი მონაცემები, რომელთა დამუშავებაც მათთვის უბრალოდ სასურველი, იაფი ან კომფორტულია და არა აუცილებელი.

ამ პრინციპიდან გამომდინარე, ასევე დაუშვებელია ისეთ მონაცემთა დამუშავება, რომელიც, სავარაუდოა, რომ მომავალში გამოგვადგება კონკრეტული/შესაძლო მიზნებით, მაგრამ ზუსტად ვერ გვეცოდინება, როდის დადგება ამის აუცილებლობა, რაში და როგორ გამოვიყენებთ მათ. ანუ არ შეიძლება მონაცემების მოპოვება და შენახვა, როცა მათი ადვილად/იაფად მოპოვების შესაძლებლობა გვაქვს. თუმცა ეს სიტუაცია უნდა განვასხვაოთ ისეთი მდგომარეობიდან, როდესაც ვიცით, კონკრეტულად რაში გამოვიყენებთ მონაცემებს, მაგრამ ზუსტად არ ვიცით, როდის. მაგალითად, ორგანიზაცია, რომლის თანამშრომლებსაც ჯანმრთელობისთვის სახიფათო სამუშაოების შესრულება უწევთ, შესაძლოა ფლობდეს ინფორმაციას თანამშრომელთა სისხლის ჯგუფის ან ჯანმრთელობასთან დაკავშირებული სხვა დეტალების შესახებ, თუმცა არ არსებობს ამ მონაცემების გამოყენების საჭიროება, არ იციან, რეალურად დასჭირდებათ თუ არა ისინი. მიუხედავად ამისა, შეიძლება მონაცემთა ამგვარი დამუშავება „მინიმიზაციის“ პრინციპთან თავსებადად ჩაითვალოს.

ისიც უნდა აღინიშნოს, რომ მიზნისადმი „ადეკვატურობისა“ და „პროპორციულობის“ მოთხოვნა არ შეიძლება გავაიგივოთ მხოლოდ „მონაცემთა მინიმიზაციასთან“. პროპორციულობა იმასაც გულისხმობს, რომ მიზნის მისაღწევად მონაცემები საკმარისი უნდა იყოს.

მიზნის მისაღწევად აუცილებელი „მონაცემთა მინიმუმის“ განსაზღვრის თვალსაზრისით პრაქტიკული მნიშვნელობის კითხვაა როდის, რა ეტაპზე უნდა მივიღოთ ამგვარი გადაწყვეტილება. მარტივი და პირდაპირი პასუხია: მონაცემთა დამუშავების ცალკეული ოპერაციის დაწყებამდე ან დაწყების პროცესში. თუმცა, წმინდა პრაქტიკული თვალსაზრისით, სასურველია, ერთმანეთისგან გამოვყოთ ორი შემთხვევა:

1. როდესაც მონაცემთა სისტემატური დამუშავების განზრახვასთან გვაქვს საქმე (მაგალითად, როცა ორგანიზაცია ახალ ბიზნესპროცესს გეგმავს, ახალ ელექტრონულ პროგრამას ავითარებს და წინასწარ ცნობილია, რომ კონკრეტული მიზნის მისაღწევად მრავალჯერადად სჭირდება მონაცემები) და

2. როდესაც პერსონალური მონაცემების დამუშავების საჭიროება დგება ცალკეულ შემთხვევებში, კონკრეტული მიზნის მისაღწევად და მას არასისტემატური ხასიათი აქვს. პირველ შემთხვევაში „აუცილებელი მონაცემების“ განსაზღვრა, რა თქმა უნდა, თავად ახალი ბიზნესპროცესის დაგეგმვის დროს უნდა მოხდეს, ახალი საქმისწარმოების პროგრამის შემუშავებამდე, რათა გადაწყვეტილება შესაბამის აქტში/ტექნიკურ დავალებაში აისახოს; მეორე შემთხვევაში კი მონაცემთა დამუშავების მიზნის მისაღწევად აუცილებელი მინიმუმი უნდა განისაზღვროს ყოველ კონკრეტულ საქმეზე/შემთხვევაში, მონაცემთა დამუშავების კონკრეტული ოპერაციის მიმართ. აქვე უნდა აღინიშნოს, რომ პერსონალურ მონაცემთა დამუშავებისას ხშირად ვაწყდებით პირველ შემთხვევას – მონაცემთა დამუშავება სისტემატურად, მრავალჯერადად ხდება ან/და მონაცემთა სუბიექტების განუსაზღვრელ წრესთან მიმართებით არსებობს მონაცემთა დამუშავების იგივე/მსგავსი მიზანი და, შესაბამისად, მონაცემთა ერთი და იგივე ოდენობაა საჭირო, რაც, თავის მხრივ, ამარტივებს პროცესს – კონკრეტული საინფორმაციო სისტემის მიზნებისთვის მონაცემთა საჭირო რაოდენობის სტანდარტიზების შესაძლებლობას იძლევა.

მიუხედავად იმისა, თუ მონაცემების დამუშავების როგორ შემთხვევასთან გვაქვს საქმე (სისტემატური-მრავალჯერადი თუ ერთჯერადი) დამმუშავებელი ყურადღებით უნდა მოეპყროს უკვე მოპოვებული და დამუშავების პროცესში მყოფი მონაცემების მინიმიზაციის საკითხს. პერიოდულად უნდა შეფასდეს დამუშავებაში მყოფი მონაცემების საჭიროება/აუცილებლობა შეცვლილი გარემოებებისა თუ უკვე მიღწეული შედეგების ფონზე.

კიდევ ერთი უაღრესად პრაქტიკული მნიშვნელობის საკითხი, რაც „მონაცემთა აუცილებელი მინიმუმის“ განსაზღვრასთან მიმართებით წამოიჭრება ქართულ პრაქტიკაში, ეს არის უკვე დამუშავების პროცესში მყოფი მონაცემები – კანონის ამოქმედებამდე (ან მის გათვალისწინებამდე) დანერგილი საინფორმაციო სისტემები, ელექტრონული პროგრამები და მონაცემთა ბაზები/არქივები. პრაქტიკაში მრავლად გვხვდება შემთხვევები, როდესაც საჯარო თუ კერძო დაწესებულებები მიზნისადმი არაპროპორციული, გადაჭარბებული მოცულობის მონაცემებს ამუშავებენ და ხშირად კრიტიკულად გააზრებული არ აქვთ ეს საკითხი, რადგან წინათ პერსონალური მონაცემების დაცვა და, შესაბამისად, მისი მინიმიზაცია მათი პრიორიტეტი და ზრუნვის საგანი არასოდეს ყოფილა. ამ საკითხზე არსებობს თეორიულად მარტივი, თუმცა შესრულების თვალსაზრისით საკმაოდ შრომატევადი გამოსავალი – მონაცემთა დამმუშავებლებმა უნდა უზრუნველყონ მათთან დამუშავებაში მყოფი მონაცემის (და დამუშავების ოპერაციების) აღწერა/ინვენტარიზაცია, კონკრეტული მიზნების განსაზღვრა

და ამ მიზნისთვის აუცილებელი მონაცემთა მინიმუმის გამოყოფა, ხოლო დანარჩენი კატეგორიის მონაცემების დამუშავების შეწყვეტა, არსებულის განადგურება ან ანონიმიზაცია.

მონაცემთა დაცვასთან დაკავშირებული ძირითადი გამოწვევები საქართველოს საჯარო სექტორში (ელექტრონული მმართველობის კონტექსტში)

საქართველოში მონაცემთა დაცვის კანონმდებლობის დანერგვაზე აქტიური მუშაობა 2014 წლიდან დაიწყო, მას შემდეგ, რაც პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი (ამჟამად სახელმწიფო ინსპექტორის სამსახური) რეალურად ამოქმედდა.

კანონის იმპლემენტაციის მიზნით საჯარო თუ კერძო ორგანიზაციებმა არაერთი აქტივობა განახორციელეს. 2014 წელს აქტიურად შეივსო და ინსპექტორის აპარატს წარედგინა ფაილური სისტემების კატალოგები, გადამზადდა და სპეციალური ტრენინგი გაიარა არაერთმა მოხელემ/დასაქმებულმა, რიგმა დაწესებულებებმა შექმნეს შიდაორგანიზაციული დოკუმენტები, დანიშნეს პერსონალურ მონაცემთა დაცვის საკითხებზე პასუხისმგებელი პირები თუ სტრუქტურული ერთეულები.

2014 წელთან შედარებით, დღეისათვის მონაცემთა დამმუშავებლებში ამაღლებულია მონაცემთა დაცვის კანონმდებლობის ცნობადობა, დაწესებულებები ცდილობენ, თავიდან აირიდონ ჯარიმა მონაცემთა დამუშავების წესების დარღვევისათვის, ფორმალურად მოაწესრიგონ მონაცემთა დამუშავების საფუძვლები, მოიპოვონ მონაცემთა სუბიექტის თანხმობა, შექმნან რიგი შიდაორგანიზაციული დოკუმენტები და ა.შ.

თუმცა, ისიც უნდა აღინიშნოს, რომ მსგავსი მიდგომა ხშირად საკითხის მხოლოდ ფრაგმენტულ მოწესრიგებას ემსახურება და თემაში გარკვეული გარე დამკვირვებლებისთვის კვლავ რჩება გარკვეული სკეპტიციზმის საფუძველი, რადგან ჯერ კიდევ არ ჩანს დაწესებულების მიერ საკითხისადმი სისტემური მიდგომა, მონაცემთა დაცვის პრინციპების ჯეროვანი გააზრება და მონაცემთა დაცვის, როგორც ყოველდღიური საქმიანობის ერთ-ერთი მნიშვნელოვანი ასპექტის დანერგვა მიმდინარე პროცესებში. ამის ნაცვლად ჩვენ ვხედავთ აღმოჩენილი/გამოვლენილი შედეგების გადაჭრის მცდელობას და არა შედეგების გამომწვევ მიზეზებთან საბრძოლველ თანმიმდევრულ ნაბიჯებს.

2019-2020 წლებში ინოვაციებისა და რეფორმების ცენტრმა (IRC) განახორციელა მონაცემთა დამუშავების 20-ზე მეტი სისტემის მონიტორინგი იმის გასარკვევად, თუ რამდენად სერიოზულად ეკიდებიან დაწესებულები მონაცემთა დაცვის საკითხს. მონიტორინგის ფარგლებში არსებული პრაქტიკა შემოწმდა როგორც მოქმედ კანონმდებლობასთან შესაბამისობის კუთხით, ისე საუკეთესო ქართული და ევროპული პრაქტიკის გათვალისწინებით.

როგორც აღნიშნული კვლევების, ისე სხვა დაკვირვებების საფუძველზე შეიძლება გამოვყოთ საჯარო დაწესებულებების მიერ მონაცემთა დამუშავების პროცესში ყველაზე გავრცელებული/მნიშვნელოვანი 10 სისუსტე.

მონაცემთა დამუშავების სისტემების (პროცესებისა და საშუალებების) ინვენტარიზაცია

მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობის უზრუნველსაყოფად ერთ-ერთი პირველი ნაბიჯი, რომელიც მონაცემთა დამმუშავებელმა უნდა გადადგას, არის მონაცემთა ინვენტარიზაცია ანუ იმის გაანალიზება, თუ სად და რა მონაცემებს აგროვებს, იყენებს თუ სხვაგვარად ამუშავებს ორგანიზაცია.

მონაცემთა ინვენტარიზაცია გულისხმობს თითოეული მონაცემისთვის იმის განსაზღვრას, თუ რა არის:

- ამ მონაცემის დამუშავების მიზანი;
- დამუშავების საფუძველი;
- ვინ არის ასეთი მონაცემების სუბიექტი;
- რა არის მონაცემების მიღების წყარო ანუ საიდან მოვიდა/შემოვიდა მონაცემები ორგანიზაციაში;
- ვინ არის პასუხისმგებელი მონაცემებზე;
- ვის შეიძლება ჰქონდეს წვდომა მონაცემებზე;
- მონაცემების შენახვის ფორმატი – ქაღალდი/ელექტრონული;
- მონაცემთა ორგანიზაციის გარეთ გადაცემის შესაძლებლობა/შემთხვევები;
- მონაცემთა შენახვის ვადა;
- მონაცემთა წაშლის/განადგურების წესი;
- სხვა.

საჯარო დაწესებულებათა მნიშვნელოვან ნაწილს მონაცემთა დაცვის მიზნებისათვის მსგავსი ინვენტარიზაცია არ აქვს ჩატარებული. შესაძლებელია, ზოგიერთ ორგანიზაციას მისი სტრუქტურის, სიდიდისა და სიმწიფის დონიდან გამომდინარე, ცალკეული პროცესებისთვის დამტკიცებული აქვს სტანდარტული წესები, შიდაორგანიზაციული თუ ანგარიშგების მიზნებისთვის აღრიცხავს მასთან შესულ და გასულ კორესპონდენციას და ა.შ., არსებულ აქტივებს ინახავს დადგენილი წესით, თუმცა, როგორც წესი, აღნიშნული ღონისძიებები არ არის გატარებული პერსონალურ მონაცემთა ინვენტარიზაციის მიზნებისთვის და გათვალისწინებული არ არის მონაცემთა დაცვის სპეციფიკა, რაც, თავის მხრივ, მონაცემთა დაცვის სტანდარტს დაბლა სწევს და კანონმდებლობასთან სათანადოდ შესაბამისობას ვერ უზრუნველყოფს.

მონაცემთა დამუშავების სისტემების ამოქმედებამდე მონაცემთა დამუშავების ზეგავლენისა და რისკების წინასწარი შეფასება

იმისთვის, რომ მონაცემთა უსაფრთხოებისათვის ადეკვატური ზომები იქნეს მიღებული და მონაცემთა დამმუშავებელმა რეალურად შეასრულოს კანონით დაკისრებული ვალდებულებები, აუცილებელია, მონაცემთა ამა თუ იმ ფორმით დამუშავების დაწყებამდე მან წინასწარ შეაფასოს მონაცემთა დამუშავებით გამოწვეული რისკები და მისი გავლენა ადამიანის ძირითად უფლებებზე. განსაკუთრებით მაშინ, თუ მონაცემთა კატეგორიის, მოცულობის მონაცემთა დამუშავების მიზნებისა და საშუალებების გათვალისწინებით, არის მაღალი რისკი.

რისკებზე დაფუძნებული მიდგომის თანახმად, ზეგავლენის შეფასების ჩატარება საჭიროა, თუ მუშავდება დიდი რაოდენობით მონაცემთა სუბიექტების განსაკუთრებული კატეგორიის მონაცემები, ხორციელდება ქცევის სისტემატური და მასშტაბური მონიტორინგი, ადამიანისთვის არსებითად მნიშვნელოვანი შედეგი დგება პროფილირების საფუძველზე და ა.შ.

მიუხედავად იმისა, რომ აღნიშნულ ვალდებულებას მოქმედი კანონმდებლობა არ ითვალისწინებს, ის ევროპაში ფართოდ გავრცელებული პრაქტიკაა და საქართველოს პარლამენტში ინიციირებული „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის პროექტიც აწესებს მსგავს მიდგომას.

დაწესებულებათა აბსოლუტურ უმრავლესობას არ აქვს ჩატარებული მონაცემთა დამუშავების ზეგავლენის შეფასება და არ აქვს იდენტიფიცირებული ის რისკები და მათთან გამკლავების გზები, რომლებიც ელექტრონულ სისტემაში მონაცემთა დამუშავებას ახლავს თან. აღნიშნული მეტად საგულისხმოა იმ სისტემებთან მიმართებით, რომელთა ინიციირებაც მოხდა და ამოქმედდა სულ ცოტა ხნის წინ, მაშინ, როდესაც მონაცემთა დაცვის შედარებით ახალი კონცეფციებიც აღარაა უცხო და ხელმიუწვდომელი მონაცემთა მსხვილი დამმუშავებლებისთვის. ჯანდაცვის საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტროს ინფორმაციით, EHR სისტემასთან მიმართებით მათ ჩატარებული აქვთ მსგავსი შეფასება, თუმცა *„ეს ყველაფერი არ არის ფორმალიზებული დოკუმენტის დონეზე, რადგან სადღეისოდ სამინისტროს არ ჰყავს ინფორმაციული უსაფრთხოების მენეჯერი“.*

მსგავსი მიდგომა, ცხადია, ვერ ჩაითვლება რეალურად გატარებულ ზომად და კანონთან თუ კარგ პრაქტიკასთან შესაბამის ღონისძიებად, რადგან შეუძლებელია, მონაცემთა დამმუშავებელმა სისტემურად და სიღრმისეულად შეაფასოს მონაცემთა დამუშავების პროცესი, დეტალურად შეაფასოს მოსალოდნელი რისკები და მათი აღრიცხვისა და დოკუმენტირების გარეშე შექმნას მათზე რეაგირების ადეკვატური მექანიზმები, რადგანაც მონაცემთა

დაცვა, მათი უსაფრთხოება და არსებულ რისკებზე რეაგირების მექანიზმები – ორგანიზაციულ-ტექნიკური ზომები – არ შეიძლება ერთჯერადი იყოს და იმისთვის, რომ ისინი ქმედითად მივიჩნიოთ, აუცილებლად განგრძობითი, დოკუმენტირებული პროცესია საჭირო.

შესაბამისად, მსგავსი მოცულობისა და მნიშვნელობის ელექტრონული სისტემის შექმნის, დანერგვისა და გაშვების დროს მნიშვნელოვანია, წინასწარ მოვიძიოთ და გამოვყოთ ადეკვატური ფინანსური თუ ადამიანური რესურსი.

მონაცემთა დამუშავების არსებული პრაქტიკის შეფასება პერსონალურ მონაცემთა დაცვის კანონმდებლობის ჭრილში

მიუხედავად იმისა, რომ ზოგიერთ უწყებას/დამმუშავებელს შექმნილი და დამტკიცებული აქვს მონაცემთა დაცვის პოლიტიკა ან/და მონაცემთა დამუშავების მარეგულირებელი და სხვა შიდაორგანიზაციული წესები, ისინი არაა საკმარისად დეტალიზებული და უწყებაში მონაცემთა დამუშავების კონკრეტულ შემთხვევებზე მორგებული. მონაცემთა დამუშავების ძირითადი სისტემები მონაცემთა დაცვის კანონმდებლობის შემოღებამდეა შემუშავებული, შესაბამისად, არც აღნიშნულ სისტემებშია იმთავითვე გათვალისწინებული მონაცემთა დაცვის საკითხები. მცირეა ისეთი შემთხვევები, როდესაც მონაცემთა დამუშავების დადგენილი პრაქტიკა საფუძვლიანად გაანალიზდა და გადაიხედა/შეიცვალა პერსონალურ მონაცემთა დაცვის კანონის მოთხოვნების გათვალისწინებით.

მონაცემთა დამუშავების მიზნებისა და საფუძვლების იდენტიფიცირება და დოკუმენტირება

დაწესებულებათა მნიშვნელოვან ნაწილს განსაზღვრული აქვს მონაცემთა დამუშავების ზოგადი მიზანი და საფუძველი და ამ თვალსაზრისით ფორმალურად შეესაბამებიან კანონმდებლობას. თუმცა მიზნებისა და საფუძვლების დაკონკრეტების ნაწილში პრობლემა იჩენს თავს. დაწესებულებათა დიდ ნაწილს დეტალურად არ აქვს იდენტიფიცირებული და დოკუმენტირებული მონაცემთა დამუშავების კონკრეტული მიზნები, საფუძვლები და კრიტიკულად არ არის გაანალიზებული მათ მიმართ მონაცემთა მოცულობა. პერსონალურ მონაცემთა დაცვის კანონმდებლობა კი სწორედ მსგავს კონკრეტიკას მოითხოვს. მონაცემები შეიძლება დამუშავდეს მხოლოდ მკაფიოდ განსაზღვრული კანონიერი მიზნის მისაღწევად, მხოლოდ იმ მოცულობით, რომელიც აუცილებელია აღნიშნული მიზნის მისაღწევად და მხოლოდ იმ შემთხვევაში, თუ მონაცემთა დამუშავების თითოეული ეპიზოდისათვის (შეგროვება, გამოყენება, შენახვა, გადაცემა და ა.შ.) არსებობს კანონით გათვალისწინებული ერთი საფუძველი მაინც. ამიტომ იმისთვის, რომ მონაცემთა დამუშავება სრულ შესაბამისობაში იყოს კანონმდებლობასთან და მონაცემთა დამმუშავებელმა აღნიშნულის დემონსტრირება შეძლოს, აუცილებელია მას დეტალურად ჰქონდეს შეფასებული და იდენტიფიცირებული მონაცემთა დამუშავების მიზანი და საფუძველი მონაცემთა თითოეული ერთეულისათვის, აღნიშნული კი შესაბამის დოკუმენტაციაში ასახოს.

მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს შორის ურთიერთობის რეგლამენტაცია კანონმდებლობის მოთხოვნათა შესაბამისად

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ადგენს მინიმალურ წესებს მონაცემთა დამმუშავებლისა და უფლებამოსილი პირის ურთიერთობებისათვის. კანონმდებლობის თანახმად, უფლებამოსილმა პირმა შეიძლება დაამუშაოს მონაცემები სამართლებრივი აქტის ან მონაცემთა დამმუშავებელთან დადებული წერილობითი ხელშეკრულების საფუძველზე, რომელიც უნდა შეესაბამებოდეს და ითვალისწინებდეს კანონის მოთხოვნებს, წესებსა და აკრძალვებს. ხოლო მონაცემთა დამმუშავებელი ვალდებულია, დარწმუნდეს აღნიშნული წესების დაცვასა და უფლებამოსილი პირის მიერ მონაცემთა უსაფრთხოებისათვის სათანადო ზომების მიღების ფაქტში. მონაცემთა დამმუშავებლის ეს ვალდებულება იქიდან გამომდინარეობს, რომ მონაცემთა დამუშავებასა და კანონის მოთხოვნების დაცვაზე კვლავ მონაცემთა დამმუშავებელია პასუხისმგებელი, მიუხედავად იმისა, რომ ფაქტობრივად მონაცემებთან შეხება უფლებამოსილ პირს აქვს.

როგორც წესი, ურთიერთობები მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს შორის არასათანადოდ არის მოწესრიგებული. რიგ შემთხვევებში საერთოდ არ არსებობს ურთიერთობების მომწესრიგებელი რამე დოკუმენტი, ან თუ არსებობს, ისინი ზოგადი და ბუნდოვანია და არ ითვალისწინებს კანონის მოთხოვნებს. ამგვარი ხელშეკრულებებით/მემორანდუმებით გათვალისწინებული არ არის კანონით დადგენილი წესები, მონაცემთა უსაფრთხოების სათანადო ზომები, მონაცემთა დამმუშავებლის მიერ პროცესის მონიტორინგის ეფექტიანი მექანიზმები და ა.შ.

მონაცემთა დამუშავების ვადების განსაზღვრა

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-4 მუხლის თანახმად, მონაცემები უნდა დამუშავდეს მხოლოდ იმ ვადით, რაც აუცილებელია მონაცემთა დამუშავების მიზნების მისაღწევად. მიზნის მიღწევის შემდეგ მონაცემები უნდა წაიშალოს/განადგურდეს.

უმეტესად ცალკეული მონაცემებისა და ასევე მთლიანად დამუშავების სისტემებისათვის განსაზღვრული არ არის კონკრეტული, კანონიერ მიზანთან შესაბამისი ვადები. ასევე არ არსებობს მონაცემთა განადგურებისა თუ დაარქივების სათანადო წესები. დაწესებულებებს უმეტეს შემთხვევაში არ აქვთ დადგენილი მონაცემთა შენახვის/დაარქივების კონკრეტული ვადები ან მონაცემთა შენახვისათვის შეუსაბამოდ ფართო დიაპაზონი აქვთ განსაზღვრული (მაგ. 1 თვიდან 3 წლამდე ვადით).

ამგვარი მიდგომები, ერთი მხრივ, მოწმობს იმას, რომ ამა თუ იმ სისტემის დანერგვისას შეფასებული და გაანალიზებული არ არის მასში დამუშავებული თითოეული მონაცემის დამუშავების მიზანი და განსაზღვრული არაა მიზნის ადეკვატური შენახვის ვადა. პრობ-

ლემურია ის საკითხიც, რომ მონაცემთა სუბიექტს არ შეუძლია განჭვრიტოს, მის შესახებ რომელი მონაცემი რა ვადით შეიძლება იქნეს შენახული.

ასევე შესაძლებელია, ცალკეულ შემთხვევებში მონაცემთა დიდი ვადით ან უვადოდ შენახვა იყოს საჭირო, თუმცა მსგავს შემთხვევაში იდენტიფიცირებული უნდა იყოს კონკრეტული საჭიროება, მონაცემთა დამუშავების საჭიროების მიზნიდან გამომდინარე კონკრეტული ვადები და მონაცემთა შენახვისა თუ განადგურების კონკრეტული წესები. თითოეული მონაცემის დამუშავების აუცილებლობის შეფასების შემდგომ უნდა გაიმიჯნოს, რომელი მონაცემები საჭიროებს ხანგრძლივი ვადით (ან მუდმივად) შენახვას და რომელი არა.

მონაცემთა ყოველი კონკრეტული წყებისათვის კრიტიკულად უნდა შეფასდეს მისი შენახვის საჭიროება, არსებობს თუ არა რამე ლეგიტიმური მიზანი მონაცემთა შემდგომი დამუშავებისათვის და მხოლოდ ასე მიიღონ გადაწყვეტილებები. აღნიშნული ინფორმაცია იოლად ხელმისაწვდომი უნდა იყოს მონაცემთა სუბიექტისთვისაც.

მონაცემთა სუბიექტის უფლებების რეალიზაციის მექანიზმების არსებობა

მონაცემთა დაცვის ფილოსოფიის ერთ-ერთი საკვანძო საკითხია მონაცემთა სუბიექტი, როგორც მონაცემთა დამუშავების ცენტრალური ფიგურა. კანონმდებლობა მონაცემთა დამმუშავებლის მხარეს მრავალ ისეთ მექანიზმსა და ვალდებულებას განსაზღვრავს, რომლებიც მონაცემთა სუბიექტის უფლებების განმტკიცებას და მის მიერ საკუთარ მონაცემებზე კონტროლის შენარჩუნებას ემსახურება. კანონმდებლობა მონაცემთა დამმუშავებელს კონკრეტული ზომების მიღებას და მონაცემთა სუბიექტის უფლების სათანადო რეალიზების ხელშეწყობას ავალდებულებს.

დაწესებულებათა უმეტესობის შემთხვევაში პრობლემურია მონაცემთა სუბიექტის უფლების რეალიზების მექანიზმები, რაც გამოიხატება არა იმდენად კონკრეტულ ფაქტებში, როდესაც სუბიექტს შეეზღუდა მონაცემთა დაცვის კანონმდებლობით გათვალისწინებული უფლებები, არამედ სისტემურ სურათში, როდესაც ეფექტიანი მექანიზმების არარსებობა, მონაცემებზე წვდომის არასათანადო აღრიცხვა და ა.შ. ქმნის საფრთხეს, მონაცემთა სუბიექტის მოთხოვნა ვერ დაკმაყოფილდეს ან მხოლოდ ნაწილობრივ დაკმაყოფილდეს.

პერსონალურ მონაცემთა დაცვისკენ მიმართული ორგანიზაციულ-ტექნიკური ზომები

მოქმედი კანონმდებლობა მონაცემთა უსაფრთხოების საკითხს მხოლოდ ერთ მუხლს უთმობს და საკმაოდ ზოგად ფორმულირებას გვთავაზობს – მონაცემთა დამმუშავებელი ვალდებულია, მიიღოს ისეთი ორგანიზაციული და ტექნიკური ზომები, რომლებიც უზრუნველყოფს მონაცემთა დაცვას შემთხვევითი ან უკანონო განადგურებისაგან, შეცვლისაგან, გამჟღავნებისაგან, მოპოვებისაგან, ნებისმიერი სხვა ფორმით უკანონო გამოყენებისა და შემთხვევითი ან უკანონო დაკარგვისაგან... ასევე, მონაცემთა უსაფრთხოებისათვის მიღე-

ბული ზომები მონაცემთა დამუშავებასთან დაკავშირებული რისკების ადეკვატური უნდა იყოს.

ამგვარი ფორმულირება, ერთი მხრივ, ბუნდოვანია და ხშირად მონაცემთა დამმუშავებლებს უჭირთ იმის ზუსტად განსაზღვრა, თუ რა კონკრეტული ზომები იქნება მათ მიერ დამუშავებულ მონაცემებთან დაკავშირებული რისკების ადეკვატური. ხოლო, მეორე მხრივ, მონაცემთა დამმუშავებლებს უქმნის უსაფუძვლო განცდას, თითქოს კანონის მოთხოვნებს სათანადოდ ასრულებენ და მათ მიერ მონაცემთა დამუშავება შეესაბამება კანონმდებლობას.

კარგი პრაქტიკის, ევროპული რეგულაციისა და ქართულ კანონმდებლობაში ინიცირებული ცვლილებების საფუძველზე შეიძლება ჩამოვთვალოთ ის მინიმალური ზომები, რომლებიც აუცილებლად უნდა მიიღოს მონაცემთა დამმუშავებელმა მონაცემთა უსაფრთხოების უზრუნველსაყოფად და რომელთა არარსებობის შემთხვევაში შეუძლებელია მონაცემთა დაცულობაზე საუბარი, მიუხედავად იმისა, კონკრეტული დარღვევა/შემთხვევა მოხდება თუ არა.

ასეთი ზომებია, მაგალითად:

- შესაბამისი პოლიტიკის დოკუმენტები;
- მონაცემთა ინვენტარიზაცია;
- მონაცემთა დამუშავების ზეგავლენის შეფასება (DPIA);
- მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნის პროცესში („Privacy by Design“) და მონაცემთა დაცვა პირველად პარამეტრად („Privacy by Default“);
- ფსევდონიმიზაცია, მონაცემებთან წვდომის აღრიცხვა, მონაცემთა ლოგირება;
- მონაცემთა დაცვის ოფიცერი;
- მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის აღრიცხვა.

მონაცემთა უსაფრთხოების უზრუნველსაყოფად აუცილებელი ორგანიზაციულ-ტექნიკური ზომების განსაზღვრისას დამმუშავებელმა და უფლებამოსილმა პირმა უნდა გაითვალისწინონ მონაცემთა კატეგორიები, მოცულობა, მონაცემთა დამუშავების მიზანი, ფორმა, საშუალებები და მონაცემთა სუბიექტის უფლებების დარღვევის შესაძლო საფრთხეები, ასევე, პერიოდულად შეაფასონ მონაცემთა უსაფრთხოების უზრუნველყოფის მიზნით მიღებული ტექნიკური და ორგანიზაციული ზომების ეფექტიანობა და, საჭიროების შემთხვევაში, უზრუნველყონ მონაცემთა უსაფრთხოების დაცვისათვის ადეკვატური ზომების მიღება ან/და არსებულის განახლება.

საქართველოში მონაცემთა დამმუშავებლების დიდ ნაწილს მონაცემთა უსაფრთხოებისათვის სათანადო და კომპლექსური ზომები არ აქვს მიღებული. საჯარო უწყებების მიერ

მიღებული უსაფრთხოების ზომები ნაკარნახევია არა მონაცემთა დაცვის სპეციფიკიდან და საჭიროებებიდან გამომდინარე, არამედ ზოგადად დაწესებულებაში სხვა მონაცემებისა თუ ფასეულობის უსაფრთხოების დაცვით.

უწყებებს ძირითადად მიღებული აქვთ ისეთი ზომები, როგორიცაა, მაგ. სისტემებთან დაშვების ავტორიზაცია, თუმცა ავტორიზაციის წესები და სტანდარტები ყოველთვის არ არის სისტემაში არსებული მონაცემების სენსიტიურობის ადეკვატური. ასევე, ხშირ შემთხვევაში, არ არსებობს მომხმარებლისა და პაროლების მართვის მომწესრიგებელი დოკუმენტი, რაც დამატებით საფრთხეს ქმნის მონაცემების გაჟონვისა და მათზე არასანქცირებული წვდომის თვალსაზრისით.

მონაცემთა უსაფრთხოებისათვის მიღებულ ზომებში შეიძლება ჩაითვალოს ფიზიკური უსაფრთხოებაც, თუმცა, როგორც უკვე აღინიშნა, ერთი მხრივ, ეს გულისხმობს ზოგად სტანდარტს შენობაში უსაფრთხოების დასაცავად და გათვალისწინებული არ არის მონაცემთა დაცვის თვალსაზრისით სენსიტიური არეები და, მეორე მხრივ, ფიზიკური უსაფრთხოება, როგორც წესი, გარედან მომავალ საფრთხეს მიემართება და ვერ იცავს ორგანიზაციას ე.წ. ინსაიდერული რისკებისაგან.

მონაცემთა დაცვის კანონმდებლობით გათვალისწინებული მონაცემთა უსაფრთხოების უზრუნველსაყოფად მისაღები ორგანიზაციული და ტექნიკური ზომები უწყებებს ძალიან ფრაგმენტულად აქვთ გათვალისწინებული. ზოგიერთ უწყებაში მიღებულია მონაცემთა ბაზებზე წვდომის ავტორიზაცია, ზოგიერთი დამმუშავებელი ახდენს მონაცემთა მიმართ შესრულებული ქმედებების ლოგირებას და ა.შ., მაგრამ უმრავლეს შემთხვევაში არ ხდება სიტუაციის დეტალური ანალიზი, სათანადო შეფასება და დამუშავებული მონაცემების ადეკვატური ზომების მიღება.

როლებისა და პასუხისმგებლობების განსაზღვრა პერსონალურ მონაცემთა დაცვის სფეროში

როგორც უკვე აღინიშნა, მონაცემთა უსაფრთხოებისათვის მისაღები ერთ-ერთი ადეკვატური ზომაა პერსონალურ მონაცემთა მიმართ უწყების შიგნით კონკრეტული როლებისა და პასუხისმგებლობების განსაზღვრა. იმის გარკვევა, საკუთარი უფლებამოსილებებიდან გამომდინარე ვის რა მონაცემებზე სჭირდება წვდომა და რა ფარგლებში. არ კმარა მონაცემთა დამუშავების კანონიერი საფუძვლის მოძიება და შესაბამისი საფუძვლის გარეშე მონაცემთა არგაცემა. მონაცემთა სათანადოდ დასაცავად აუცილებელია, სისტემის შიგნითაც იყოს განაწილებული როლები და უფლებამოსილებების ფარგლები.

მონაცემთა დამუშავების სისტემათა უმეტესობას პერსონალურ მონაცემებზე წვდომის საკითხები არ აქვს დოკუმენტირებული და შესაბამისად რეგლამენტირებული. პრაქტიკულად სისტემებში არსებობს მომხმარებელთა განსხვავებული ტიპები, თუმცა არაა დოკუმენტი, რომელიც დაადგენს, რომელ თანამშრომელს რომელი უფლებამოსილების ფარგლებში

რა მონაცემებზე შეიძლება ჰქონდეს წვდომა და რა მოქმედებების განხორციელება შეუძლია ამ წვდომის ფარგლებში. მსგავსი მიდგომა კი ზრდის მონაცემებზე არასანქცირებული წვდომის, გადაჭარბებული დამუშავებისა და გაჟონვის რისკებს.

ადამიანური რესურსის მომზადების დონე/სისტემური მიდგომა

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონისა და ინსპექტორის სამსახურის (ყოფილი პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატი) ამოქმედების შემდეგ, სამსახური რეგულარულ ტრენინგებს სთავაზობს სხვადასხვა დაინტერესებულ პირებს. ასევე, მრავალი სასწავლო ცენტრის სწავლების გეგმა ითვალისწინებს პერსონალურ მონაცემთა დაცვის საკითხებს.

მიუხედავად იმისა, რომ ასეთი ზოგადი ხასიათის ტრენინგები თითქმის ყველა უწყებაში ტარდება და/ან ჩატარებულა, მას ვერ მივიჩნევთ საჯარო დაწესებულებათა მიერ სისტემური მიდგომის ნაწილად და თანამშრომელთა სათანადო გადამზადებად.

ადამიანებს, რომელთაც მუდმივად აქვთ შეხება პერსონალურ მონაცემებთან და რომელთათვისაც პერსონალური, მათ შორის განსაკუთრებული კატეგორიის მონაცემების დამუშავება ყოველდღიური საქმიანობის ნაწილია, მნიშვნელოვანია კარგად ჰქონდეთ გაცნობიერებული პერსონალურ მონაცემთა დაცვის მნიშვნელობა, მონაცემთა დამუშავების პრინციპები, საკუთარი უფლება-მოვალეობები და მონაცემთა დაცვასთან დაკავშირებული სხვა საკითხები.

ამისთვის მნიშვნელოვანია, ორგანიზაციის/უწყების შიგნით ხელმისაწვდომი იყოს პერსონალურ მონაცემთა დამუშავების კონკრეტული გზამკვლევები და სასწავლო გეგმები, რომლებშიც გათვალისწინებული იქნება სამსახურის სპეციფიკა და მონაცემთა დაცვის ზოგადი პრინციპები, დებულებები „გადმოთარგმნილი“ და მორგებული იქნება თანამშრომლის ყოველდღიურ საქმიანობაზე.

სპეციალიზებული სასწავლო კურსები/მასალები, როგორც წესი, პრაქტიკაში არ გვხვდება და არც თანამშრომელთა სავალდებულო გადამზადების ნაწილს წარმოადგენს.

პერსონალურ მონაცემთა დაცვასთან დაკავშირებული საკითხები, რომლებიც ელექტრონული მმართველობის პროექტების დაგეგმვისა და იმპლემენტაციისას უნდა გავითვალისწინოთ

პერსონალურ მონაცემთა დაცვასთან დაკავშირებული კონკრეტული ამოცანების განხილვამდე მნიშვნელოვანია, ხაზი გავუსვათ იმ დამოკიდებულებას, რომელიც მონაცემთა დაცვის საკითხს სჭირდება ელექტრონული მმართველობის პროექტის ხელმძღვანელისა თუ დაწესებულების მაღალი რგოლის მენეჯერისგან.

პირველი, რაც ელექტრონული მმართველობის პროექტის/სისტემის ინიციატორმა უნდა გააკეთოს, თავად პერსონალურ მონაცემთა დაცვის საკითხის აღიარებაა – იმის გაცნობიერება, რომ ასეთი განზომილება არსებობს და საკითხი სერიოზულ დამოკიდებულებას მოითხოვს. შესაძლოა ეს მოწოდება ბანალურ ჭეშმარიტებად ჩანდეს, მაგრამ თუ თვალს გადავავლებთ საქართველოში ელექტრონულ მმართველობაში გამოყენებული სისტემების მონაცემთა დაცვის პრობლემატიკას, დავრწმუნდებით, რომ უმრავლეს შემთხვევაში პრობლემა სწორედ საკითხის არაღიარებითა და მისთვის არასაკმარისი მნიშვნელობის მინიჭებით იწყება.

ხშირად პერსონალურ მონაცემთა დაცვა მცდარად მიაჩნიათ მცირე საკითხად და დეტალად სხვა მრავალ წვრილმანს შორის, რომელთაც ორგანიზაციის IT დეველოპერი ან/და იურისტი მოაგვარებს პროექტის იმპლემენტაციის რომელიღაც ეტაპზე.

რეალურად კი ესაა საკითხი, რომლის „მოგვარებას“ სჭირდება მნიშვნელოვანი გადაწყვეტილებების მიღება ზედა მენეჯმენტის მიერ, პროექტის ინიციირებისა და იმპლემენტაციის ადრეულ სტადიებზე. საექსპერტო პერსონალთან ერთად ზედა მენეჯმენტის ჩართულობაც მნიშვნელოვანია, რადგან თემატური ცოდნის გარდა მისაღები გადაწყვეტილებები შეიძლება ბიზნესმოდელის შინაარსს, ბიზნესპროცესების შესაძლო ცვლილებას, გარკვეული ფინანსური დანახარჯების ზრდას და მისთ. უკავშირდებოდეს.

მონაცემთა დამუშავების მიზნის განსაზღვრა

ელექტრონული მმართველობის პროექტის გუნდმა, მათ შორის მონაცემთა დაცვის საკითხზე პასუხისმგებელმა კონსულტანტმა/მრჩეველმა კარგად უნდა იცოდნენ თავად პროექტის მიზნები და, აქედან გამომდინარე, ცალკეულ მონაცემთა დამუშავების მიზანი. ერთი შეხედვით ეს თავისთავად ცხადია და სხვაგვარად წარმოუდგენელია მსგავსი ინიციატივების დანერგვაზე მუშაობა, თუმცა პრაქტიკა საპირისპიროს მოწმობს – ხშირად იწყება ელექტრონული მმართველობის სხვადასხვა მასშტაბის პროექტები, რომელთა კონკრეტულ ამოცანებს ორგანიზატორები „გზადაგზა“ არკვევენ ან/და გარკვეულ მიზნები მხოლოდ „ნაგულისხმებია“, თუმცა პროექტის გუნდში არასაკმარისად იმსჯელეს დაინტერესებულ მხარეებთან და ეტაპობრივად ირკვევა, რომ მოლოდინები ერთმანეთს სცდება.

როდესაც პერსონალურ მონაცემთა დაცვის კონტექსტში დამუშავების მიზნების განსაზღვრაზეა საუბარი, რა თქმა უნდა, იგულისხმება არა მხოლოდ ზოგადი იდეა და მიზნები, როგორებიცაა მომსახურების გაუმჯობესება, კომფორტული დისტანციური მომსახურება, მომხმარებელთა უსაფრთხოება და ა.შ., არამედ სისტემისა თუ ახალი სერვისის თანმდევი უფრო კონკრეტული მიზნები და ამოცანები.

აღნიშნულის გარეშე შეუძლებელი იქნება მონაცემთა დამუშავების კონკრეტული მიზნების იდენტიფიცირება და იმის განსაზღვრა, თუ ამ სისტემისთვის მონაცემთა რა აუცილებელი მინიმუმის შეგროვება/დამუშავებაა საჭირო. როგორც ზემოთ განვიხილეთ, მონაცემთა

დაცვის უმნიშვნელოვანეს პრინციპს წარმოადგენს დამუშავების მინიმიზაცია, რაც გულისხმობს, რომ უნდა დამუშავდეს მხოლოდ ის მონაცემები, მხოლოდ იმ ფორმით და იმ ვადით, რომლებიც მიზნის მისაღწევადაა საჭირო.

ეს ყველაფერი ერთი შეხედვით მარტივი ჭეშმარიტებაა, მაგრამ ქართულ პრაქტიკაში იშვიათად გვაქვს შემთხვევები, როცა ეს საკითხი ბოლომდეა გააზრებული და პირიქით, არის შემთხვევები, როდესაც მუშავდება ისეთი პერსონალური მონაცემები, რომელთა გამოყენებაც მიზნის მისაღწევად აუცილებელი არაა, თუმცა ამ საკითხზე არავის უფიქრია, ან იფიქრეს, მაგრამ აღმოჩნდა, რომ ელექტრონული პროგრამა იმგვარადაა დაწერილი, რომ საჭირო და არასაჭირო მონაცემების გამიჯვნა ვერ ხდება. მაგალითად, ზოგჯერ ელექტრონული სისტემის მომხმარებელთა ნაწილს წვდომა აქვს იმ ინფორმაციაზე, რაც მას ამოცანების შესასრულებლად არ სჭირდება ანდა ერთი ორგანიზაციიდან მეორისთვის ელექტრონული სერვისის მიწოდებისას საჭირო (კანონმდებლობით გათვალისწინებულ) პერსონალურ მონაცემს თან მისდევს სხვა ისეთი მონაცემიც, რომლის გადაცემის სამართლებრივი საფუძველი/ფუნქციური საჭიროება არ არსებობს, თუმცა ტექნიკურად მათი გამიჯვნა შეუძლებელია და პროგრამულ ცვლილებას მოითხოვს. ეს ყველაფერი კი ხშირად იმითაა განპირობებული, რომ სისტემის დაგეგმვის ეტაპზე მონაცემთა დამუშავების მიზნები და მონაცემთა დაცვის თვალსაზრისით სხვა მნიშვნელოვანი ასპექტები გათვალისწინებული არ არის.

მონაცემთა დამუშავების ფარგლები და მონაცემთა სუბიექტების კატეგორიის განსაზღვრა

პერსონალურ მონაცემთა დაცვასთან დაკავშირებულ ვალდებულებებსა და შესაბამის განსახორციელებელ ამოცანებს/აქტივობებს მნიშვნელოვნად განსაზღვრავს ის, თუ სად და ვის შესახებ იგეგმება მონაცემების შეგროვება და დამუშავება. მაგალითად, მნიშვნელოვანია, რომ ელექტრონული მმართველობის პროექტის ინიციირების საწყის ფაზაშივე გაირკვეს, ხომ არ იგეგმება არასრულწლოვანთა შესახებ მონაცემების დამუშავება ან/და ახალი სისტემის (პროდუქტის/სერვისის) მიზანი ევროკავშირის ტერიტორიაზე მყოფი ადამიანების (საქართველოს მოქალაქეების ან უცხოელების) შესახებ მონაცემების დამუშავება ხომ არაა, ტერიტორიულად სად იწყება მონაცემთა შეგროვება და ხომ არ იგეგმება მონაცემთა გადაცემა სხვა სახელმწიფოში. ზემოაღნიშნული საკითხების წინასწარ გააზრება მნიშვნელოვანია, ვინაიდან ეს გავლენას ახდენს როგორც გამოსაყენებელი სამართლებრივი ნორმებისა და სტანდარტების განსაზღვრაზე, ისე კონკრეტული ორგანიზაციულ-ტექნიკური საშუალებებისა და გადაწყვეტების შერჩევაზე, რისი დანერგვაც, მონაცემთა დაცვის კანონმდებლობის მოთხოვნებიდან გამომდინარე, შესაძლოა მონაცემთა დამმუშავებელს მოუწიოს.

მონაცემთა კატეგორიის განსაზღვრა

მნიშვნელოვანია, ელექტრონული სისტემის/სერვისის მფლობელმა ანუ მონაცემთა დამმუშავებელმა წინასწარ განსაზღვროს მონაცემთა ყველა ის კატეგორია, რომელიც მის ხელთ არსებული სისტემის საშუალებით დამუშავდება. აღნიშნულის გაკეთება აუცილებელია, რადგან კანონმდებლობა სხვადასხვა კატეგორიის პერსონალური მონაცემების მიმართ, დაცვის სხვადასხვა რეჟიმს ადგენს – განსხვავდება მონაცემთა დამუშავების საფუძვლებიც და, ამასთან, მონაცემთა კატეგორია ხშირად გავლენას ახდენს გასატარებელ ორგანიზაციულ-ტექნიკურ ზომებზე.

მონაცემთა დამუშავების საფუძვლების განსაზღვრა

ხშირად ესა თუ ის ელექტრონული სისტემა/სერვისი/პროდუქტი სუბიექტთა ფართო წრის შესახებ სხვადასხვა კატეგორიის პერსონალური მონაცემების დამუშავებას ითვალისწინებს, რასაც ასევე საფუძველი შეიძლება ჰქონდეს. მნიშვნელოვანია, მონაცემთა დამმუშავებელმა ელექტრონული სისტემის დაგეგმვისას ზუსტად განსაზღვროს, მონაცემთა დამუშავების რომელი ოპერაციისა და რომელი კატეგორიის მონაცემისთვის კანონით გათვალისწინებული დამუშავების რომელი საფუძველი გააჩნია. საკმაოდ გავრცელებულ შეცდომას ვაწყდებით შემთხვევისას, როდესაც დამმუშავებელი პერსონალურ მონაცემებზე განსახორციელებელი ერთი ოპერაციისთვის რელევანტურ სამართლებრივ საფუძველს არასწორად იყენებს იმავე მონაცემებთან დაკავშირებით განხორციელებული სხვა ოპერაციების მიმართ. მაგალითად, მონაცემთა შეგროვებისა და გადაწყვეტილებების მისაღებად მათი გამოყენების კანონიერი საფუძვლის არსებობა (ანუ მონაცემების კანონიერად ფლობა) თავისთავად არ ნიშნავს იმას, რომ სხვა ორგანიზაციებისთვის მათი გადაცემის საფუძველი არსებობს, ეს კი პრაქტიკაში ყოველთვის გათვალისწინებული არ არის. ელექტრონული მმართველობის სახელმწიფო სისტემებთან მიმართებით ასევე გავრცელებულ შეცდომას წარმოადგენს „მონაცემთა სუბიექტის თანხმობის“ განხილვა მონაცემთა დამუშავების საფუძვლად – როგორც წესი, საჯარო სექტორში მონაცემთა დამუშავების სხვა საფუძვლები არსებობს და სუბიექტის თანხმობა რელევანტურ საფუძვლად არ მიიჩნევა.

მონაცემთა დამუშავების ვადების განსაზღვრა

მონაცემთა დამუშავების მიზნებიდან გამომდინარე, აუცილებელია მონაცემთა დამუშავების ვადების წინასწარ განსაზღვრა, ან თუკი დამუშავების ვადები დადგენილია კანონმდებლობით, აღნიშნულის იდენტიფიცირება და ელექტრონული მმართველობის სისტემის/სერვისის დიზაინისას მისი გათვალისწინება. თუ მონაცემთა დამუშავების ვადები წინასწარ განისაზღვრება, შესაძლებელია ელექტრონული სისტემის დიზაინისას გაითვალისწინონ და შეიმუშაონ, მაგალითად, ისეთი ფუნქციონალი, რომელიც შესაბამისი ვადის დადგომისას ავტომატურ რეჟიმში უზრუნველყოფს მონაცემთა დამუშავების შეწყვეტას, მონაცემთა განსაზღვრული ნაწილის განადგურებას ან მათ დეპერსონალიზაციას.

მონაცემთა დაცვაზე გავლენის შეფასება

მიუხედავად იმისა, რომ საქართველოს კანონმდებლობით მონაცემთა დაცვაზე გავლენის შეფასება (DPIA) ჯერჯერობით სავალდებულო არ არის, ხოლო იმ ქვეყნებშიც კი, სადაც სავალდებულოა, ყოველთვის აუცილებლობას არ წარმოადგენს მისი ჩატარება. ელექტრონული მმართველობის პროექტები (სერვისები/პროდუქტები) სწორედ ის სფეროა, სადაც DPIA-ის ჩატარება უკიდურესად მნიშვნელოვანი და რეკომენდებულია. ცხადია, DPIA-ის ჩატარება მარტივი ამოცანა არ არის და გარკვეულ კომპეტენციას მოითხოვს, მით უმეტეს, საქართველოში მსგავსი გამოცდილება ძალიან მწირია. თუმცა საკითხის მნიშვნელობის გაცნობიერების შემთხვევაში შესაძლებელია ამ კომპეტენციის განვითარება და პრაქტიკაში გამოყენება. დღეისათვის ხელმისაწვდომია უამრავი ფასიანი ონლაინკურსი ინგლისურ ენაზე, ასევე უფასო პრაქტიკული რეკომენდაციები და ინსტრუმენტები (Tool kits) სხვადასხვა ქვეყნების მონაცემთა დაცვის საზედამხედველო ორგანიზაციების ვებგვერდებზე (https://ico.org.uk / https://www.priv.gc.ca/en)

მონაცემთა სუბიექტების ინფორმირება და მათი უფლებების რეალიზების მექანიზმები

პერსონალურ მონაცემთა დაცვის კანონმდებლობის ცენტრში მონაცემთა სუბიექტია – თანამედროვე კანონმდებლობა სწორედ სუბიექტის უფლებებსა და მათი რეალიზაციის გზებზეა ფოკუსირებული. მონაცემთა სუბიექტის უფლებების დაცვას მხოლოდ უმოქმედობით და მათ „არდარღვევით“ ვერ მივაღწევთ. მონაცემთა დაცვის კანონმდებლობა, მათ შორის ქართული კანონი ითვალისწინებს მონაცემთა სუბიექტის ისეთ უფლებებს, რომელთა რეალიზება ორგანიზაციულ-ტექნიკური თვალსაზრისით ყოველთვის მარტივი არაა, თუ შესაბამისი ორგანიზაცია ამაზე წინასწარ, სისტემის დიზაინისას არ იზრუნებს.

ამ თვალსაზრისით, რაზეც უპირველეს ყოვლისა უნდა დაფიქრდეს მონაცემთა დამმუშავებელი, დგება საკითხი, თუ როდის და რა გზით უნდა მიეწოდოს ინფორმაცია მონაცემთა სუბიექტს მისი პერსონალური მონაცემების დამუშავების თაობაზე, როგორ უზრუნველყოს მონაცემთა სუბიექტების ყველა კატეგორიისთვის დროულად და გასაგები ფორმით ინფორმაციის მიწოდება მონაცემთა დამუშავების მიზნებსა და ფარგლებზე, რათა მათ რეალურად განჭვრიტონ, რა ბედი ეწევა თავიანთ მონაცემებს. ასევე გასათვალისწინებელია, რომ მონაცემთა სუბიექტის ისეთი უფლებები, როგორებიცაა, მაგალითად, ინფორმაციის მიღების უფლება იმაზე, თუ ვის, როდის და რის საფუძველზე გადაეცა მისი მონაცემები და ტექნიკურ გადაწყვეტებს საჭიროებს, რასაც ელექტრონული სისტემის დაგეგმვისას უნდა მიექცეს ყურადღება.

ურთიერთობის მოწესრიგება „უფლებამოსილ პირებთან“

ელექტრონული სერვისების შექმნასა და მუშაობაში, როგორც წესი, მონაწილეობს არა მხოლოდ სერვისის შემქმნელი/მიმწოდებელი ერთი პასუხისმგებელი ორგანიზაცია, არა-

მედ სხვა ორგანიზაციებიც, რომლებიც გარკვეულ მომსახურებას აწვდიან ელექტრონული სერვისის მფლობელს. მაგალითად, საჯარო დაწესებულებათა ნაწილს, რომლებიც კონკრეტული ელექტრონული სერვისების მიწოდებაზე არიან პასუხისმგებელნი და ამ სერვისის შინაარსს განსაზღვრავენ, არ გააჩნიათ საკუთარი ICT ინფრასტრუქტურა (სერვერული ცენტრი ან/და პროგრამული უზრუნველყოფა) და სხვა დაწესებულების მომსახურებას იყენებენ. იგულისხმება ისეთი შემთხვევა, როდესაც ფორმალურ-სამართლებრივად სერვისის მფლობელად განსაზღვრულია ერთი დაწესებულება; ის განსაზღვრავს სერვისის კონფიგურაციას, მონაცემთა დამუშავების მიზნებსა და ფარგლებს, ხოლო შესაბამისი ამოცანების ტექნიკურ რეალიზაციაში დახმარებას უწევს ანუ მომსახურებას აწვდის სხვა საჯარო თუ კერძო დაწესებულება. ამ უკანასკნელს საქართველოს კანონი პერსონალურ მონაცემთა დაცვის შესახებ „უფლებამოსილ პირს“ უწოდებს და ადგენს გარკვეულ წესებს, რომელთა დაცვაც აუცილებელია სერვისის მფლობელს, ანუ მონაცემთა დამმუშავებელსა და უფლებამოსილ პირს შორის ურთიერთობისას. მაგალითად, აუცილებელია, წერილობითი ხელშეკრულების გაფორმება მონაცემთა დამუშავების დაწყებამდე. შესაბამისად, ნებისმიერი ელექტრონული სერვისის გაშვებამდე უნდა გაირკვეს პროცესში მონაწილე ორგანიზაციების სტატუსი პერსონალურ მონაცემთა დაცვის კანონმდებლობის ჭრილში – ვინაა მონაცემთა დამმუშავებელი, ვინ შეიძლება ჩაითვალოს მონაცემთა თანადამმუშავებლად და ვინ წარმოადგენს „უფლებამოსილ პირს“.

პერსონალურ მონაცემთა დაცვასთან დაკავშირებული როლებისა და პასუხისმგებლობების განსაზღვრა

ელექტრონული მმართველობის პროექტის შემმუშავებელ/დამნერგავ ორგანიზაციას აუცილებლად უნდა ჰქონდეს განსაზღვრული როლები და პასუხისმგებლობები მონაცემთა დაცვის მიმართულებით. პერსონალურ მონაცემთა დაცვასთან დაკავშირებული ამოცანები თავისთავად არ შესრულდება. არასწორია წარმოდგენა, თითქოს მონაცემთა დაცვა უბრალოდ წესების არ დარღვევას ნიშნავს და საამისოდ პასიური მოქმედება/უმოქმედობა საკმარისია. მნიშვნელოვანია განისაზღვროს კონკრეტული პასუხისმგებლობები – მაგალითად, ვინ უნდა შეაფასოს ახალი ელექტრონული სერვისი თუ პროდუქტი მონაცემთა დაცვის კანონმდებლობის ჭრილში, ვინ ამუშავებს მონაცემებს და ვინაა პასუხისმგებელი დაცვასთან დაკავშირებული აქტივობების დოკუმენტირებაზე, რათა შესაძლებელი იყოს შესაბამისობის დადგენა და „ანგარიშვალდებულების პრინციპის“ დაცვა; ვინ აგებს პასუხს მონაცემთა სუბიექტის განცხადებების განხილვასა თუ სხვა უფლებების რეალიზებაზე, სისტემაში ცვლილებების ინიციირებისას ვინ უნდა უზრუნველყოს მონაცემთა დაცვის ოფიცრის ან/და სხვა პირთა ინფორმირება, რათა დაგეგმილი ცვლილებები წინასწარ შეფასდეს; ვინ აწვდის ინფორმაციას თანამშრომლებს მონაცემთა დაცვის საკითხებზე და ა.შ.

მონაცემთა დამუშავების პროცესთან დაკავშირებული თანამშრომლების ინფორმირება/ტრენინგი

უდავოა, რომ ელექტრონული სერვისების შექმნით/მიწოდებით დაკავებული ნებისმიერი დაწესებულების თანამშრომლებს პერსონალურ მონაცემთა დაცვის სფეროში გარკვეული ინფორმაცია და კომპეტენცია სჭირდებათ. საკითხთა წრე და კომპეტენციის სიღრმე, რომელიც ამა თუ იმ დაწესებულების თანამშრომელს მოეთხოვება მონაცემთა დაცვის სფეროში, დამოკიდებულია როგორც დაწესებულების საქმიანობის სპეციფიკაზე, ისე კონკრეტული თანამშრომლის როლსა და პასუხისმგებლობებზე. ზოგადი საორიენტაციო ტრენინგი – „one size fits all“ პრინციპით, რომელიც ყველა თანამშრომელმა შეიძლება გაიაროს, – ცხადია, სასურველია და „სულ არაფერს“ სჯობია, თუმცა, როგორც წესი, არ კმარა. ამ თვალსაზრისით, ელექტრონული სერვისების მიმწოდებელმა დაწესებულებამ უპირველეს ყოვლისა, უნდა განსაზღვროს საჭირო კომპეტენციები და ექსპერტის დონე და, შესაბამისად, დაგეგმოს სხვადასხვა დონის ტრენინგ პროგრამები/მოდულები, რომელთაც პერიოდულად სხვადასხვა კატეგორიის თანამშრომლებისთვის ჩაატარებს/დაუკვეთავს.