სახელმწიფო ინსპექტორის სამსახური

სახელმწიფო ინსპექტორის სამსახურის რეკომენდაციები

COVID-19-ის წინააღმდეგ ბრძოლის პროცესში პერსონალურ მონაცემთა დამუშავება

2020 წელი

Norwegian Ministry of Foreign Affairs

Empowered lives.
Resilient nations.

რეკომენდაციები შექმნილია ნორვეგიის მთავრობისა და გაეროს განვითარების პროგრამის (UNDP) მხარდაჭერით. მის შინაარსზე სრულად პასუხისმგებელია სახელმწიფო ინსპექტორის სამსახური და შესაძლოა, რომ იგი არ გამოხატავდეს ნორვეგიის მთავრობისა და გაეროს განვითარების პროგრამის შეხედულებებს.

COVID-19-ის გავრცელების მასშტაბის ზრდასთან ერთად, საზოგადოებაში ჩნდება კითხვები ვირუსთან ბრძოლის პროცესში პერსონალური მონაცემების დაცვასთან დაკავშირებით.

შესაბამისად, სახელმწიფო ინსპექტორის სამსახურმა COVID-19-ის წინააღმდეგ ბრძოლის პროცესში პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებით რეკომენდაციები შეიმუშავა, რომელიც მიზნად ისახავს კონფიდენციალური ინფორმაციის მართვის პროცესში ორგანიზაციების დახმარებას.

რეკომენდაციაში მოცემულია განმარტებები შემდეგ საკითხებზე:

- ჯანდაცვის დაწესებულებების მიერ პერსონალურ მონაცემთა დამუშავება;
- დამსაქმებელთა მიერ დასაქმებულთა ჯანმრთელობის შესახებ მონაცემთა დამუშავება;
- დისტანციური შეხვედრებისა და სწავლების პროცესში პერსონალური მონაცემების დამუშავება;
- დისტანციური მუშაობისას სამსახურებრივი (პერსონალური) მონაცემების დაცვა და უსაფრთხოება.

სახელმწიფო ინსპექტორის სამსახური
STATE INSPECTOR'S SERVICE

ჯანდაცვის დაწესებულებების მიერ მონაცემთა დამუშავება

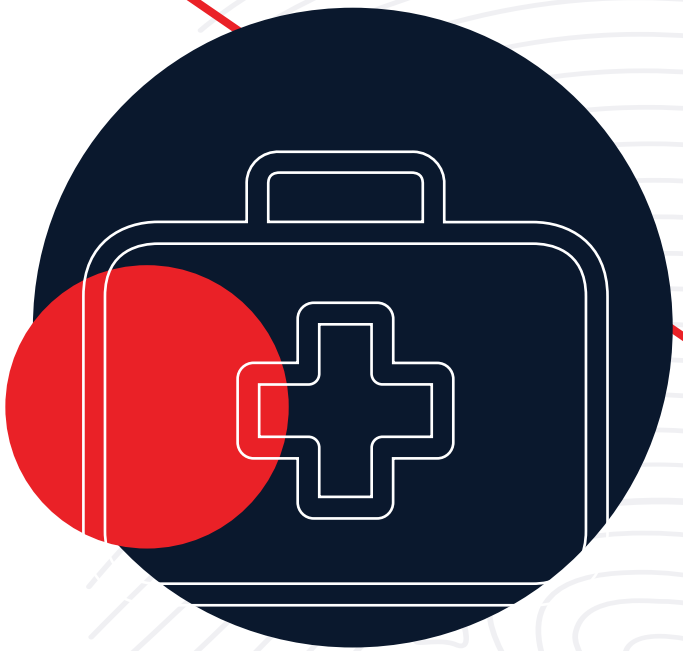
საზოგადოებრივი ჯანდაცვის დაწესებულებები, მოქმედი კანონმდებლობის საფუძველზე, აგროვებენ და ამუშავებენ სხვადასხვა პერსონალურ მონაცემებს, რაც აუცილებელია ჯანმრთელობის დაცვის სისტემის მართვისა და ფუნქციონირებისთვის.

ვირუსის გავრცელების წინააღმდეგ ბრძოლის პროცესში, ჯანდაცვის დაწესებულებებს უწევთ ინფიცირებულ ან/და შესაძლო ინფიცირებულ პირთა შესახებ მეტი მოცულობით მონაცემების შეგროვება, ვიდრე სტანდარტულ შემთხვევებში (მაგალითად, აგროვებენ ინფორმაციას მოქალაქეთა საზღვარგარეთ მოგზაურობის, სამუშაო ადგილის, ახლო კონტაქტში მყოფი პირების შესახებ), რაც არსებული საჭიროებიდან გამომდინარეობს და არ ეწინააღმდეგება კანონმდებლობას.

პანდემიის შესახებ საზოგადოების ინფორმირებისა და სამედიცინო კონსულტაციების გაწევის მიზნით, დასაშვებია საინფორმაციო შეტყობინებების გაგზავნა სატელეკომუნიკაციო და თანამედროვე ტექნოლოგიების საშუალებით.

გასათვალისწინებელია, რომ ასეთი სიტუაციების დროს, იზრდება შეცდომაში შემყვანი და ე. წ. „თაღლითური შეტყობინებების“ მიღების რისკი. შესაბამისად, მნიშვნელოვანია, მოქალაქეები დაეყრდნონ მხოლოდ ოფიციალური ორგანოებიდან მიღებულ ინფორმაციას.

ვირუსით ინფიცირებულ, შესაძლო ინფიცირებულ ან/და მათთან კონტაქტში მყოფ პირთა ვინაობის (სახელის, გვარის) საჯაროდ გავრცელება, როგორც წესი, აუცილებელი არ არის და საზოგადოებრივი ინტერესის დასაკმაყოფილებლად საკმარისია მათ შესახებ არაიდენტიფიცირებადი ფორმით ინფორმაციის გავრცელება (მოქალაქეობა, ეთნიკური კუთვნილება, ასაკი, სამუშაო ადგილი, მათი გადაადგილების მარშრუტი და ა.შ.). აღნიშნულ პირთა ვინაობის შესახებ მონაცემების გასაჯაროება და მესამე პირთათვის გამჟღავნება დასაშვებია იმ მოცულობითა და იმ ფარგლებში, რაც აუცილებელია დაავადების პრევენციის, კონტროლისა და მართვისათვის.



დამსაქმებელი ორგანიზაციების მიერ დასაქმებულთა მონაცემების დამუშავება

დასაქმებულთათვის უსაფრთხო გარემოს უზრუნველყოფის პარალელურად, დამსაქმებლები ცდილობენ შეინარჩუნონ საქმიანობის უწყვეტობა.

კანონმდებლობის თანახმად, დამსაქმებლებს დასაქმებულთა დაინფიცირების შესახებ ინფორმაციის შეგროვება შეუძლიათ დასაქმებულთა ნების მიუხედავად, თუ ეს ემსახურება უსაფრთხო შრომითი გარემოს უზრუნველყოფას ან/და ემსახურება ჯანმრთელობის დაცვის სისტემის მართვას.

დასაშვებია დამსაქმებელმა შეაგროვოს შემდეგი ინფორმაცია: დასაქმებული სტუმრობდა თუ არა ვირუსის გავრცელების მაღალ რისკის შემცველ ქვეყანას, აქვს თუ არა დასაქმებულს ვირუსის სიმპტომები, ჰქონდა თუ არა კონტაქტი ვირუსით დაინფიცირებულ პირ(ებ)თან.

დასაქმებულის დაინფიცირების შესახებ ეჭვის შემთხვევაში დამსაქმებელმა უნდა მიმართოს შესაბამის ჯანდაცვის უწყებას და დაექვემდებაროს მის მითითებებს.

დამსაქმებლის მიერ, დასაქმებულის დაინფიცირების შესახებ, ინფორმაციის სხვა დასაქმებულებისათვის გამჟღავნება დასაშვებია, თუ ეს აუცილებელია დასაქმებულთან კონტაქტში მყოფი პირების გამოსავლენად ან/და ვირუსის შემდგომი გავრცელების პრევენციისთვის.

მოპოვებული მონაცემები დამსაქმებელმა უნდა შეინახოს იმ ვადით, რაც აუცილებელია მის კომპეტენციას მიკუთვნებული ღონისძიებების განხორციელებისთვის. შემდგომ ეს მონაცემები უნდა წაიშალოს, განადგურდეს ან შენახულ იქნას პირის იდენტიფიცირების გამომრიცხავი ფორმით.

დისტანციური სწავლება და შეხვედრები

დისტანციურ სწავლებაზე გადავიდნენ საგანმანათლებლო დაწესებულებებიც (სკოლები, უნივერსიტეტები), ასევე, ხშირია დისტანციურად შეხვედრების გამართვის პრეცედენტები.

სოციალურ ქსელებში ვრცელდება ონლაინ სასწავლო პროცესის, ონლაინ შეხვედრების ამსახველი (მათ შორის, იუმორისტული) ფოტო-ვიდეო მასალა.

ონლაინ შეხვედრების, ონლაინ-სწავლების ამსახველი მასალა (ფოტო, ვიდეო გამოსახულება) წარმოადგენს პირის პერსონალურ მონაცემებს, რაც უნდა იქნეს გათვალისწინებული მათი გასაჯაროებისას.

არასრულწლოვნის მონაცემების ინტერნეტში ყველასთვის ხელმისაწვდომი ფორმით გასაჯაროებამ შესაძლოა არასასურველი ზეგავლენა მოახდინოს არასრულწლოვანზე (გახდეს ბულინგის ან სხვა სახის არასასურველი მოპყრობის ობიექტი).

შესაბამისად, საგანმანათლებლო დაწესებულებები, ამ დაწესებულებებში დასაქმებული პირები, ასევე, არასრულწლოვანი პირების მშობლები და ოჯახის წევრები, მეტი პასუხისმგებლობით უნდა მოეკიდონ ბავშვების მონაცემების გასაჯაროებას და იმოქმედონ არასრულწლოვნის საუკეთესო ინტერესების გათვალისწინებით.

დისტანციური შეხვედრების გამართვისათვის, შეგიძლიათ გამოიყენოთ თანამედროვე კოლაბორაციული კომუნიკაციის სისტემები (მაგალითად, Webex, Zoom, Teams და ა.შ.).

Webex Meetings | zoom | Microsoft Teams

სახელმწიფო ინსპექტორის სამსახური
STATE INSPECTOR'S SERVICE

დისტანციურად მუშაობისას მონაცემთა დამუშავება

ორგანიზაციათა უმეტესობამ უკვე მიმართა დისტანციურად მუშაობის რეჟიმს. თანამედროვე ტექნოლოგიებმა დისტანციურად მუშაობა მარტივი გახადა, თუმცა ასეთ დროს დღის წესრიგში დგება სამსახურებრივი ინფორმაციის კონფიდენციალობის დაცვისა და უსაფრთხოების საკითხი.

დისტანციურად მუშაობისას გასათვალისწინებელი გარემოებები:

- სახლიდან დისტანციურად მუშაობისას სასურველია გამოყენებულ იქნეს სამსახურის კომპიუტერი;
- თუ საჭიროა სახლის კომპიუტერიდან სამსახურის კომპიუტერში დისტანციური წვდომის საშუალებებით შესვლა, ამისათვის აუცილებლად უნდა იქნეს გამოყენებული თანამედროვე და განახლებული პროგრამები;
- საკუთარ კომპიუტერში რეგულარულად უნდა განახლდეს ოპერაციული სისტემები (MS Windows, MacOS);
- აუცილებელია კომპიუტერში შესვლის პაროლის დაყენება;
- იმ ელექტრონულ სისტემებში შესვლისთვის, რომელზეც წვდომა ინდივიდუალური მომხმარებლის სახელით არის შესაძლებელი, უმჯობესია გამოყენებულ იქნეს რთული და კომპლექსური პაროლი (რომელიც შეიცავს არანაკლებ 10 სიმბოლოს, დიდ და პატარა ლათინურ ასოებს, ციფრებს და სპეციალურ სიმბოლოებს. მაგ.: #,$, &, @ და ა.შ.). ასევე, სადაც ეს შესაძლებელია, გამოყენებულ უნდა იქნეს ორ ფაქტორიანი ავთენტიფიკაციის მექანიზმები (მომხმარებლის სახელთან ერთად, პაროლი და დამატებითი ერთჯერად კოდი);
- ერთიდაიგივე პაროლი არ უნდა იქნეს გამოყენებული სხვადასხვა სისტემებში შესვლისათვის;
- სამსახურის შიდა ელექტრონულ რესურსებთან წვდომისათვის გამოყენებული უნდა იქნეს მხოლოდ დაშიფრული VPN კავშირის საშუალებები;

- გამოყენებული უნდა იქნეს ანტივირუსული პროგრამები, თუნდაც უფასო ვერსიები;
- სასურველია მონაცემების სარეზერვო ასლების გაკეთება ან მნიშვნელოვანი დოკუმენტების და მონაცემების სამსახურის სერვერზე შენახვა;
- უნდა დაიშიფროს კონფიდენციალური მონაცემები, თუნდაც უფასო შიფრაციის პროგრამების გამოყენებით (მაგალითად, VeraCrypt, BitLocker და ა.შ.);
- არ უნდა იქნეს გამოყენებული უცხო USB მონაცემთა მატარებლები;
- დაცული უნდა იქნას კომპიუტერის ფიზიკური უსაფრთხოება (დასაქმებულმა იგი არ უნდა დატოვოს უყურადღებოდ სხვადასხვა ადგილზე).

ასევე, დასაქმებულმა უნდა უზრუნველყოს სახლის უკაბელო ქსელური მოწყობილობის უსაფრთხოება. კერძოდ:

- სახლის უკაბელო ქსელური მოწყობილობის მართვისათვის გამოყოფილი მომხმარებლის პაროლი არ უნდა იყოს სხვისთვის ცნობილი;
- შესაძლებლობის შემთხვევაში, უმჯობესია ინტერნეტიდან შეიზღუდოს უკაბელო ქსელური მოწყობილობის სამართავ პანელზე წვდომა;
- უკაბელო ქსელური კავშირისათვის გამოყენებული შიფრაციის მეთოდები სასურველია იყოს თანამდეროვე (მაგალითად, WPA2 ან WPA3);
- სახლის უკაბელო ქსელურ მოწყობილობასთან დაკავშირების პაროლი უნდა იყოს კომპლექსური და არანაკლებ 16 სიმბოლოსგან შემდგარი;
- პერიოდულად უნდა შეიცვალოს უკაბელო ქსელის მოწყობილობასთან დაკავშირების პაროლი.

დამატებით უნდა აღინიშნოს, რომ პანდემიით გამოწვეული ვითარებით სარგებლობენ ჰაკერები.

მსოფლიოში ბევრი ცრუ ე.წ. „ფიშინგ“ საიტია შექმნილი, სადაც განთავსებულია ვირუსის გავრცელების სტატისტიკური მონაცემები და რომლებზეც შესვლის შემდგომ შესაძლებელია კომპიუტერებიდან მონაცემების მოპარვა. შესაბამისად, რეკომენდებულია ვირუსის გავრცელების სტატისტიკური მონაცემების მხოლოდ ოფიციალურ ან საინფორმაციო სააგენტოებისა და მედია ორგანიზაციების საიტებზე დათვალიერება.

ასევე, ძალიან მომატებულია ელ-ფოსტით გაგზავნილი ცრუ ე.წ. „ფიშინგ“ წერილების რაოდენობა. ამა თუ იმ ცნობილი ორგანიზაციის ან ადამიანის სახელით ცრუ შეტყობინებები იგზავნება კონფიდენციალური ან პერსონალური ინფორმაციის მოპარვის მიზნით.

საფრთხის შემცველია უცნობი ორგანიზაციების და პირების მიერ გამოგზავნილ წერილებში მიმაგრებული ფაილები. შესაბამისად, მიბმული ფაილები არ უნდა გაიხსნას, სანამ მომხმარებელი არ დარწმუნდება გამომგზავნი ორგანიზაციის ან/და პირის კეთილსინდისიერებასა და რეალურობაში.

სახელმწიფო
ინსპექტორის
სამსახური