პერსონალურ მონაცემთა დაცვა

ლექცია 2

თამარ ქურდაძე

პერსონალურ მონაცემთა დაცვის და ინფორმაციული უსაფრთხოების სამართალსა და პრაქტიკაში დამკვიდრებული ძირითადი ცნებების მიმოხილვა

- ინფორმაციული უსაფრთხოების შესახებ საქართველოს კანონი
- https://matsne.gov.ge/ka/document/view/1679424?publication=5

ყურადღება მიაქციეთ შემდეგ მუხლებს:

- მუხლი 2
- მუხლი 6
- მუხლი 7
- მუხლი 8
- მუხლი 8’1
- მუხლი 9

პერსონალური მონაცემების დაცვა და ინფორმაციის უსაფრთხოება თანამედროვე ციფრული ეპოქის კრიტიკული ასპექტებია. კანონები და პრაქტიკა ამ სფეროში ეტაპობრივად განვითარდა, პერსონალური ინფორმაციის დაცვისა და მონაცემთა უსაფრთხოების უზრუნველყოფის მიზნით. ქვემოთ მოცემულია რამდენიმე ძირითადი კონცეფციის მიმოხილვა, რომელიც დადგენილია პერსონალური მონაცემების დაცვისა და ინფორმაციული უსაფრთხოების კანონმდებლობასა და პრაქტიკაში:

- **პერსონალური მონაცემები:** პერსონალური მონაცემები არის ნებისმიერ ინფორმაციას, რომელსაც შეუძლია პიროვნების იდენტიფიცირება, პირდაპირ ან ირიბად. ეს შეიძლება შეიცავდეს სახელებს, მისამართებს, ტელეფონის ნომრებს, ელფოსტის მისამართებს და კიდევ უფრო სენსიტიურ ინფორმაციას, როგორიცაა ბიომეტრიული მონაცემები ან ფინანსური ჩანაწერები.
- **მონაცემთა სუბიექტი:** მონაცემთა სუბიექტი არის ინდივიდი, რომელსაც ეკუთვნის პერსონალური მონაცემები. მათ აქვთ უფლებები თავიანთ მონაცემებზე, მათ შორის უფლება იცოდნენ რა მონაცემები გროვდება, როგორ გამოიყენება და მოითხოვონ მისი წაშლა.
- მონაცემთა მაკონტროლებელი: მონაცემთა მაკონტროლებელი არის ორგანო, რომელიც განსაზღვრავს პერსონალური მონაცემების დამუშავების მიზნებსა და საშუალებებს. ისინი პასუხისმგებელნი არიან მონაცემთა დაცვის შესაბამისობის უზრუნველყოფაზე.
- **მონაცემთა დამმუშავებელი:** მონაცემთა დამმუშავებელი არის ორგანო, რომელიც ამუშავებს პერსონალურ მონაცემებს მონაცემთა მაკონტროლებლის სახელით. დამმუშავებლები ასევე ექვემდებარებიან მონაცემთა დაცვის კანონებს და უნდა უზრუნველყონ მათ მიერ დამუშავებული მონაცემების უსაფრთხოება.

თანხმობა: მონაცემთა დაცვის კანონმდებლობა ხშირად მოითხოვს, რომ პირებმა უზრუნველყონ ინფორმირებული და მკაფიო თანხმობა მათი მონაცემების დამუშავებამდე. თანხმობა უნდა იყოს თავისუფლად გაცემული, კონკრეტული და საჭიროებისამებრ გაუქმებადი.

მიზნის შეზღუდვა: პერსონალური მონაცემები უნდა შეგროვდეს კონკრეტული, ლეგიტიმური მიზნებისთვის და არ იქნას გამოყენებული სხვა მიზნებისთვის დამატებითი თანხმობის მიღების გარეშე.

მონაცემთა მინიმიზაცია: უნდა შეგროვდეს და დამუშავდეს მხოლოდ პერსონალური მონაცემების მინიმალური რაოდენობა, რომელიც აუცილებელია კონკრეტული მიზნის შესასრულებლად. ზედმეტი ან შეუსაბამო მონაცემები არ უნდა იყოს შენახული.

მონაცემთა უსაფრთხოება: ორგანიზაციებმა უნდა განახორციელონ შესაბამისი ტექნიკური და ორგანიზაციული ზომები, რათა დაიცვან პერსონალური მონაცემები არაავტორიზებული წვდომისგან, გამჟღავნების, ცვლილებისა და განადგურებისგან. ეს მოიცავს დაშიფვრას, წვდომის კონტროლს და უსაფრთხოების რეგულარულ აუდიტს.

კონფიდენციალურობა დიზაინით: ეს კონცეფცია ხაზს უსვამს იმას, რომ მონაცემთა დაცვა და უსაფრთხოება თავიდანვე უნდა იყოს ჩაშენებული სისტემებსა და პროცესებში.

მონაცემთა დარღვევის შესახებ შეტყობინება: მონაცემთა დაცვის მრავალი კანონი მოითხოვს ორგანიზაციებს, რომ აცნობონ როგორც მონაცემთა სუბიექტებს, ასევე ხელისუფლებას მონაცემთა დარღვევის შემთხვევაში, განსაკუთრებით თუ ეს დარღვევა საფრთხეს უქმნის ინდივიდთა უფლებებსა და თავისუფლებებს.

მონაცემთა დაცვაზე ზემოქმედების შეფასება - Data Protection Impact Assessment (DPIA): ორგანიზაციებს შეიძლება დასჭირდეთ DPIA-ების ჩატარება, რათა შეაფასონ პოტენციური რისკები მონაცემთა სუბიექტებისთვის პერსონალური მონაცემების დამუშავებისას, განსაკუთრებით ახალი ტექნოლოგიების გამოყენებისას ან სენსიტიური მონაცემების დამუშავებისას.

მონაცემთა ტრანსსასაზღვრო გადაცემა: პერსონალური მონაცემების საერთაშორისო საზღვრებს შორის გადაცემა ექვემდებარება სპეციფიკურ რეგულაციას და ორგანიზაციებს შეიძლება დასჭირდეთ უზრუნველყონ მონაცემთა დაცვის სტანდარტების დაცვა ასეთი გადაცემისას.

მონაცემთა სუბიექტის უფლებები: პირებს აქვთ სხვადასხვა უფლებები, როგორიცაა მათ მონაცემებზე წვდომის, უზუსტობების გამოსწორების, მონაცემების წაშლის (დავიწყების უფლება) და მათი მონაცემების სერვისებს შორის პორტაბელობის უფლება.

ანგარიშვალდებულება და ჩანაწერები: ორგანიზაციები ვალდებულნი არიან აწარმოონ ჩანაწერები მონაცემთა დამუშავების საქმიანობის შესახებ და აჩვენონ მონაცემთა დაცვის რეგულაციების დაცვა.

ჯარიმები: მონაცემთა დაცვის კანონების შეუსრულებლობამ შეიძლება გამოიწვიოს მნიშვნელოვანი ჯარიმები ორგანიზაციებისთვის.

General Data Protection Regulation GDPR: მონაცემთა დაცვის ზოგადი რეგულაცია არის მონაცემთა დაცვის ერთ-ერთი ყველაზე ყოვლისმომცველი და ფართოდ აღიარებული კანონი, რომელიც გამოიყენება ევროკავშირში და მთელ მსოფლიოში ორგანიზაციებზე, რომლებიც ამუშავებენ ევროკავშირის მოქალაქეების მონაცემებს.

California Consumer Privacy Act - CCPA: კალიფორნიის მომხმარებელთა კონფიდენციალურობის აქტი არის კონფიდენციალურობის სახელმწიფო კანონი შეერთებულ შტატებში, რომელიც უზრუნველყოფს კალიფორნიის მაცხოვრებლებს უფლებებს მათ პერსონალურ მონაცემებზე.

Health Insurance Portability and Accountability Act - HIPAA: ჯანმრთელობის დაზღვევის პორტაბელურობისა და ანგარიშვალდებულების აქტი არეგულირებს ჯანდაცვის შესახებ მონაცემების კონფიდენციალურობას და უსაფრთხოებას შეერთებულ შტატებში.

National Institute of Standards and Technology - კიბერუსაფრთხოების ჩარჩოები: NIST კიბერუსაფრთხოების ჩარჩოები იძლევა მითითებებს ორგანიზაციებისთვის, რათა გააძლიერონ თავიანთი კიბერუსაფრთხოების პრაქტიკა.

მონაცემთა ეთიკა: იურიდიული შესაბამისობის გარდა, ორგანიზაციები უფრო მეტად უნდა განიხილონ მონაცემთა შეგროვებისა და გამოყენების ეთიკური შედეგები.

დავალება:
სლაიდი
კანონი ინფორმაციული უსაფრთხოების შესახებ