პერსონალური მონაცემების დაცვა ონლაინ ვაჭრობის პროცესში

სახელმწიფო
ინსპექტორის
სამსახური

რეკომენდაციები

USAID
FROM THE AMERICAN PEOPLE

დემოკრატიული მმართველობის ინიციატივა

თემატური რეკომენდაციები COVID-19-ით გამოწვეული პანდემიის დროს პერსონალურ მონაცემთა მართვაზე

PHOTO CREDIT TETRA TECH

თარიღი: 20 იანვარი, 2022
წინამდებარე დოკუმენტი შემუშავებულია ამერიკის შეერთებული შტატების (აშშ) საერთაშორისო განვითარების სააგენტოს (USAID) მიერ. დოკუმენტი მომზადდა Tetra Tech-ის მხარდაჭერით.

ავტორი: შპს „იუაი“ – ტატო ჩანტლაძე, ელენე სულხანიშვილი, გიორგი ცინცქილაძე, გვანცა ჯიშიაშვილი

სარჩევი

რეკომენდაციები სავაჭრო ორგანიზაციებისთვის ონლაინ ვაჭრობისას პერსონალურ მონაცემთა დამუშავების თაობაზე 1

1. შესავალი 1
2. ტერმინთა განმარტება 2
3. ძირითადი წესები 3
4. მონაცემთა დამუშავების პროცესი ონლაინ ვაჭრობისას 4
5. პერსონალურ მონაცემთა პირდაპირი მარკეტინგის მიზნებისთვის დამუშავება 8
6. პერსონალურ მონაცემთა დამუშავება უფლებამოსილი პირის მეშვეობით 9
7. ონლაინ ვაჭრობისას მომხმარებლის უფლებები და მათი რეალიზაციის მექანიზმები 10
8. უსაფრთხოების დაცვა 11
9. ონლაინ ვაჭრობისას პერსონალურ მონაცემთა კანონიერად დამუშავების დამხმარე საშუალებები 21

დანართი 1: მომხმარებლის თანხმობის ფორმა 25

დანართი 2: მზა ჩანაწერების ნიმუში 26

დანართი 3: საკონტროლო სია 27

რეკომენდაციები მომხმარებლებისთვის ონლაინ ვაჭრობისას პერსონალურ მონაცემთა დამუშავების თაობაზე 29

1. შესავალი 29
2. ტერმინთა განმარტება 30
3. ძირითადი წესები 30
4. პერსონალურ მონაცემთა დამუშავების პროცესი ონლაინ ვაჭრობისას 31
5. პერსონალურ მონაცემთა პირდაპირი მარკეტინგის მიზნებისთვის დამუშავება 33
6. ონლაინ ვაჭრობისას მომხმარებლების უფლებები და მათი რეალიზაციის მექანიზმები 34
7. ონლაინ ვაჭრობისას პერსონალურ მონაცემთა კანონიერად დამუშავების დამხმარე საშუალებები 35
8. უსაფრთხოების დაცვა 36

რეკომენდაციები სავაჭრო ორგანიზაციებისთვის ონლაინ ვაჭრობისას პერსონალურ მონაცემთა დამუშავების თაობაზე

1. შესავალი

ახალი კორონავირუსით („COVID-19“) გამოწვეული პანდემიის პირობებში ციფრული ეკონომიკა და ონლაინ ვაჭრობა კიდევ უფრო განვითარდა. შესაბამისად, გაიზარდა ონლაინ ვაჭრობის პროცესში მომხმარებელთა პერსონალური მონაცემების დამუშავების რისკები.

მოცემული რეკომენდაციების მიზანია სავაჭრო ორგანიზაციებს მიეწოდოთ საბაზისო ინფორმაცია, როგორ დაამუშაონ პერსონალური მონაცემები ონლაინ ვაჭრობისას კანონმდებლობის მინიმალური სტანდარტების გათვალისწინებით. საკანონმდებლო მოთხოვნების დაკმაყოფილების შემთხვევაში სავაჭრო ორგანიზაციები თავიდან აიცილებენ კანონდარღვევებსა და ჯარიმებს. გარდა ამისა, რეკომენდაციების გათვალისწინებით, სავაჭრო ორგანიზაციები კიდევ უფრო დაუახლოვდებიან საერთაშორისო საუკეთესო პრაქტიკას ონლაინ ვაჭრობისას პერსონალური მონაცემების დამუშავების კუთხით. ამით, სავაჭრო ორგანიზაციები აიმაღლებენ რეპუტაციას და გახდებიან უფრო კონკურენტუნარიანი სხვა ორგანიზაციებთან შედარებით.

მოცემული რეკომენდაციები შემუშავებულია საქართველოს კანონმდებლობის მოთხოვნებისა და საუკეთესო პრაქტიკის გათვალისწინებით. სავაჭრო ორგანიზაციებს, რომლებიც ევროკავშირში მყოფ პირთა პერსონალურ მონაცემებს ამუშავებენ (ან მათზე სხვაგვარად ვრცელდება GDPR-ის[1] მოქმედება), დამატებით შესაძლოა, მოეთხოვოთ GDPR-თან შესაბამისობა. ასეთ შემთხვევაში რეკომენდებულია, რომ სავაჭრო ორგანიზაციები დეტალურად გაეცნონ GDPR-ის მოთხოვნებს.

რეკომენდაციები საინფორმაციო ხასიათისაა. სავაჭრო ორგანიზაციები თავად არიან პასუხისმგებელნი პროცედურების შემუშავებასა და კანონმდებლობასთან შესაბამისობაზე. პროცედურების დანერგვისას საყურადღებოა, მათ შორის, სავაჭრო ორგანიზაციების საქმიანობის კონკრეტული მახასიათებლები და მომხმარებლების პერსონალურ მონაცემთა დამუშავების შინაარსი. აღნიშნული კი ყოველ კონკრეტულ შემთხვევაში ინდივიდუალურად უნდა შეფასდეს.

რეკომენდაციებს თან ახლავს მაგალითები, რომლებიც არ არის ამომწურავი და მოცემულია მხოლოდ საილუსტრაციოდ.

[1] ევროპარლამენტისა და ევროკავშირის საბჭოს 2016 წლის 27 აპრილის რეგულაცია (EU) 2016/679 პერსონალურ მონაცემთა დამუშავებისას ფიზიკურ პირთა დაცვის და ასეთი მონაცემების თავისუფალი მიმოცვლის შესახებ (მონაცემთა დაცვის ძირითადი რეგულაცია).

2. ტერმინთა განმარტება

2.1. პერსონალური მონაცემი

ნებისმიერი ინფორმაცია მომხმარებლის შესახებ პერსონალური მონაცემია. მაგალითად:

- სახელი და გვარი.
- დაბადების თარიღი.
- პირადი ნომერი.
- ტელეფონის ნომერი.
- საცხოვრებელი მისამართი.
- ელექტრონული ფოსტის მისამართი.
- IP მისამართი.
- საბარათე მონაცემები.
- ვებგვერდზე სტუმრობის ფაქტი და მასზე გატარებული დრო.
- კომპიუტერული მოწყობილობის ტიპი.
- საოპერაციო სისტემა.
- ბრაუზერი.

2.2. პერსონალური მონაცემის დამუშავება

მომხმარებლის პერსონალური მონაცემის მიმართ განხორციელებული ნებისმიერი მოქმედება პერსონალური მონაცემის დამუშავებაა. მაგალითად:

- მომხმარებლის ვებგვერდზე რეგისტრაციის მიზნით მისი ელექტრონული ფოსტის, პაროლის, სახელისა და გვარის მითითება.
- მომხმარებლის მიერ შეკვეთის განსანთავსებლად მისი საბარათე მონაცემების ასახვა.
- მომხმარებლისთვის პროდუქციის/მომსახურების მისაწოდებლად მისი საცხოვრებელი მისამართის მონაცემის გამოყენება.
- მომხმარებლისთვის მარკეტინგული შეტყობინების გაგზავნა ტელეფონის ნომერზე ან ელექტრონულ ფოსტაზე.
- მომხმარებლის მიერ ვებგვერდზე გატარებული დროის ნახვა.
- მომხმარებლის მიერ ვებგვერდზე მოძიებული ინფორმაციის ნახვა.

3. ძირითადი წესები

პერსონალურ მონაცემთა დასაცავად ოთხ ძირითად გარემოებას უნდა მიაქციოთ ყურადღება. ესენია:

- არსებობს თუ არა პერსონალურ მონაცემთა დამუშავების საფუძველი (მაგალითად: მომხმარებლის თანხმობა).
- შეესაბამება თუ არა ონლაინ ვაჭრობისას მოთხოვნილი, შენახული, გამოყენებული, გაგზავნილი პერსონალური მონაცემები პერსონალურ მონაცემთა დამუშავების პრინციპებს (მაგალითად: ვადა, მიზანი).
- უზრუნველყოფილია თუ არა პერსონალურ მონაცემთა უსაფრთხოება ანუ ის ორგანიზაციულ-ტექნიკური ზომები, რომლებიც მომხმარებლებს, პერსონალური მონაცემების შემთხვევითი და უკანონო გამჟღავნებისგან იცავს.
- რეალიზებული და ხელმისაწვდომია თუ არა მომხმარებლებისთვის თავიანთი უფლებები (მაგალითად: შესწორების, განახლების, შეცვლის, ინფორმირების და სხვა უფლებები).

საქართველოს კანონმდებლობა (მათ შორის, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი) ოთხივე საკითხს დეტალურად აწესრიგებს - ამომწურავად განსაზღვრავს საფუძვლებს, პრინციპებს, ადგენს ვადებს, უფლებების კონკრეტულ ჩამონათვალს და სხვა.

ონლაინ ვაჭრობის პროცესში უნდა:

- დარწმუნდეთ, რომ პერსონალური მონაცემების დამუშავება გჭირდებათ ონლაინ ვაჭრობის მიზნით.
  - მაგალითად, გამოიყენოთ მომხმარებლის საცხოვრებელი მისამართი შეკვეთის მისატანად.
- დაამუშაოთ პერსონალური მონაცემები ონლაინ ვაჭრობისთვის საჭირო მოცულობით.
  - მაგალითად, დაამუშაოთ მომხმარებლის სახელი და გვარი მისი ონლაინ შეკვეთის გასაფორმებლად.
- დარწმუნდეთ, რომ თქვენ მიერ ონლაინ ვაჭრობისას შენახული პერსონალური მონაცემები არის ნამდვილი და ზუსტი.
  - მაგალითად, არ შეიყვანოთ მომხმარებლის მცდარი ელექტრონული ფოსტა ვებგვერდის მომხმარებელთა სიაში.
- განაახლოთ მომხმარებლის პერსონალური მონაცემები, რომლებიც შეიცვალა.
  - მაგალითად, ამ მიზნით მომხმარებლებს მისცეთ საშუალება, განაახლონ თავიანთი პირადი ინფორმაცია ვებგვერდზე (ტელეფონის ნომერი, მისამართი, ელექტრონული ფოსტა, პაროლი).
- შეინახოთ მომხმარებლის პერსონალური მონაცემები ონლაინ ვაჭრობისთვის საჭირო ვადით.
  - მაგალითად, ელექტრონული სისტემიდან წაშალოთ მომხმარებლის საბანკო ანგარიშის მონაცემები მის მიერ შეკვეთის განთავსების შემდეგ.

- დაბლოკოთ, წაშალოთ ან გაანადგუროთ მომხმარებლის პერსონალური მონაცემები, რომლებიც აღარ გჭირდებათ ან შეინახოთ ისეთი ფორმით, რომ მომხმარებლის ამოცნობა შეუძლებელი იყოს.
  - მაგალითად, განახორციელოთ მომხმარებლის პერსონალური მონაცემების დეპერსონალიზება - იდენტიფიცირებადი პირადი ინფორმაცია (მაგალითად, სახელი და გვარი) შეცვალოთ ინიციალებით.
  - მაგალითად, მომხმარებელს მისცეთ საშუალება თავად წაშალოს ვებგვერდიდან საკუთარი პროფილი.

მნიშვნელოვანია	დაშვებულია
დაიცვათ ყველა ზემოთ ჩამოთვლილი წესი ერთდროულად პერსონალური მონაცემების დამუშავებისას.	დაამუშაოთ მომხმარებლის პერსონალური მონაცემები ონლაინ ვაჭრობისას მისთვის მომსახურების გასაწევად.
დაუშვებელია	**დაუშვებელია**
არ გქონდეთ განსაზღვრული პერსონალური მონაცემების შენახვის კონკრეტული ვადები.	მოითხოვოთ ონლაინ ვაჭრობისთვის მომხმარებლის ისეთი პერსონალური მონაცემი, რომელიც მისი იდენტიფიკაციისათვის ან მომსახურების გასაწევად საჭირო არ არის, მაგალითად, რელიგიური შეხედულება.

4. მონაცემთა დამუშავების პროცესი ონლაინ ვაჭრობისას

4.1. ელექტრონულ პლატფორმებზე რეგისტრაცია/ავტორიზაცია/პროფილი/უკუკავშირი

სავაჭრო ორგანიზაციებში ონლაინ ვაჭრობის პროცესი უმეტეს შემთხვევაში შემდეგია:

ვიზიტი ვებგვერდზე - მომხმარებელი სტუმრობს სავაჭრო ორგანიზაციის ვებგვერდს.

რეგისტრაცია - მომხმარებელი სასურველი პროდუქციის/მომსახურების შეძენის მიზნით რეგისტრირდება სავაჭრო ორგანიზაციის ვებგვერდზე და ავსებს შესაბამის ფორმას.

პროფილის შექმნა - რეგისტრაციისას საჭირო ფორმის შევსების შემდეგ იქმნება მომხმარებლის პროფილი.

მომსახურების/პროდუქციის შეძენა - მომხმარებელი ირჩევს სასურველ მომსახურებას/პროდუქციას და მათ შესაძენად დამატებით ავსებს თავის საბარათე მონაცემებს.

შეკვეთის მიწოდება - სავაჭრო ორგანიზაცია მომხმარებელს აწვდის სასურველ პროდუქციას/მომსახურებას. აღნიშნული შესაძლოა ასევე მოიაზრებდეს საკურიერო მომსახურების მეშვეობით მომხმარებლის მისამართზე პროდუქციის მიტანას.

უკუკავშირი - მომხმარებლებს შეუძლიათ ნებისმიერი კითხვის შემთხვევაში მიმართონ სავაჭრო ორგანიზაციას მათ ვებგვერდზე მითითებულ ნომერზე, ჩატში, ან ელექტრონულ ფოსტაზე.

4.2. ონლაინ ვაჭრობისას დამუშავებულ პერსონალურ მონაცემთა კატეგორიები

ონლაინ ვაჭრობის პროცესში სავაჭრო ორგანიზაციების მიერ ძირითადად მუშავდება მომხმარებელთა შემდეგი კატეგორიის მონაცემები: საიდენტიფიკაციო მონაცემები, საკონტაქტო ინფორმაცია, საბანკო მონაცემები, ვებგვერდზე განხორციელებული მოქმედებები.

საიდენტიფიკაციო მონაცემები - მომხმარებლები სავაჭრო ორგანიზაციის ვებგვერდზე რეგისტრაციისათვის უთითებენ საკუთარ სახელსა და გვარს, ასევე პროდუქციის შეძენის/მომსახურების მიღების მიზნით უთითებენ პირად ნომერს.

საკონტაქტო მონაცემები - მომხმარებლები სავაჭრო ორგანიზაციის ვებგვერდზე რეგისტრაციისათვის უთითებენ საკუთარ ელექტრონულ ფოსტასა და პაროლს, რომლითაც შეძლებენ ვებგვერდზე შესვლას და სასურველი პროდუქციის შეძენას/მომსახურების მიღებას. ამასთან, პროდუქციის/მომსახურების მისაღებად შეჰყავთ თავიანთი საცხოვრებელი ადგილის მისამართი და ტელეფონის ნომერი.

ვებგვერდზე განხორციელებული მოქმედებები - სავაჭრო ორგანიზაციები სხვადასხვა ელექტრონული პლატფორმის მეშვეობით აღრიცხავენ მომხმარებლების მიერ ვებგვერდზე განხორციელებულ მოქმედებებს, ასევე ვებგვერდზე სტუმრობის დროს, IP მისამართს, კომპიუტერული მოწყობილობის ტიპს, საოპერაციო სისტემასა და ბრაუზერს.

გარდა ზემოაღნიშნულისა, საყურადღებოა, რომ ონლაინ ვაჭრობისას ზოგიერთ პერსონალურ მონაცემზე მოქმედებს დაცვის უფრო მაღალი სტანდარტი. ასეთ პერსონალურ მონაცემებს კანონმდებლობა განსაკუთრებული კატეგორიის მონაცემებად მოიხსენიებს. მაგალითად:

- მომხმარებლის ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცია.
- მომხმარებლის ნასამართლობასთან, ადმინისტრაციულ პატიმრობასთან, საპროცესო გარიგებასთან დაკავშირებული ინფორმაცია.
- მომხმარებლის რელიგიური შეხედულებები.
- მომხმარებლის პოლიტიკური შეხედულებები.
- მომხმარებლის სქესობრივი ცხოვრება.
- მომხმარებლის ეთნიკური და რასობრივი კუთვნილების შესახებ ინფორმაცია.

განსაკუთრებული კატეგორიის მონაცემების დამუშავება შეგიძლიათ მხოლოდ გამონაკლის შემთხვევებში, მაგალითად, მომხმარებლის წერილობითი თანხმობით ან თუ ეს აუცილებელია მომხმარებლის სასიცოცხლო ინტერესების დაცვისთვის, და სხვ.

მნიშვნელოვანია	დაუშვებელია
გამოიჩინოთ მომეტებული ყურადღება ონლაინ ვაჭრობისას განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისას და მაქსიმალურად დაიცვათ მომხმარებელთა პერსონალური მონაცემები.	დაავალდებულოთ მომხმარებელი მოგაწოდოთ საკუთარი ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცია.

დაუშვებელია
გაასაჯაროოთ ან მესამე პირებს გაუმჟღავნოთ მომხმარებლის განსაკუთრებული კატეგორიის მონაცემები მისი თანხმობის გარეშე.

4.3. მომხმარებელთა ინფორმირება

ონლაინ ვაჭრობისას მნიშვნელოვანია თითოეული მომხმარებელი სათანადოდ იყოს ინფორმირებული თუ რა ქმედებები ხორციელდება მისი პერსონალური მონაცემების მიმართ. ამისთვის საუკეთესო საშუალებაა ვებგვერდზე ვიზიტისთანავე მათთვის პერსონალური მონაცემების დამუშავების პოლიტიკის (ე.წ. „კონფიდენციალურობის პოლიტიკის“) მიწოდება. აღნიშნულ პოლიტიკაში დეტალურად, მომხმარებლებისთვის გასაგებ ენაზე იქნება განსაზღვრული ყველა პროცესი, რომელიც მიმდინარეობს მომხმარებელთა პერსონალურ მონაცემებთან დაკავშირებით.

ამ კონტექსტში საყურადღებოა მომხმარებელთა ინფორმირება მზა ჩანაწერების (ე.წ. „Cookies“) მეშვეობით პერსონალურ მონაცემთა დამუშავების შესახებ. მზა ჩანაწერი ტექსტური ფაილია, რომელიც ავტომატურად იქმნება ვებგვერდზე ვიზიტის, მასზე არჩეული პარამეტრების, განთავსებული სარეგისტრაციო ინფორმაციის და ისტორიის (მაგალითად, ხშირად ნანახი პროდუქციის შესახებ) შესანახად. მზა ჩანაწერების საშუალებით ხდება მომხმარებლის მიერ მოძიებული ინფორმაციისა და ვებგვერდების დამახსოვრება, მომხმარებლის ქცევის და ინტერესების შესწავლა და აღნიშნულზე დაფუძნებით მისთვის სასურველი პროდუქტების/სერვისების ავტომატურ რეჟიმში შეთავაზება.

მზა ჩანაწერების მიმართ სრულად ვრცელდება პერსონალურ მონაცემთა დამუშავებისას გასათვალისწინებელი სხვა მოთხოვნები. კერძოდ, მომხმარებლებს უნდა ჰქონდეთ ნათელი და კონკრეტული ინფორმაცია რა პერსონალური მონაცემები მუშავდება და რა არის მათი დამუშავების მიზანი. მომხმარებლებს უნდა ჰქონდეთ შესაძლებლობა, უარი თქვან მზა ჩანაწერების დამუშავებაზე.

შესაბამისად, სიფრთხილე უნდა გამოიჩინოთ მზა ჩანაწერების დამუშავებისას და უნდა მიაწოდოთ მომხმარებლებს ინფორმაცია რაც შეიძლება ნათელ, გასაგებ ენაზე, რათა მათ მკაფიოდ აღიქვან თუ როგორ დამუშავდება მათი პერსონალური მონაცემები და რა უფლებები აქვთ. ასეთი ინფორმაციის მიწოდებისას შესაძლებელია გამოყენებულ იქნას რაც შეიძლება მარტივი ენა, სიმბოლოები თუ სურათები.

მომხმარებელთა ინფორმირება მათი ვებგვერდზე ვიზიტისთანავე ერთ-ერთი საუკეთესო საშუალება იქნება პერსონალურ მონაცემთა დამუშავების სწორი პრაქტიკის დანერგვისთვის.

დაშვებულია

მიაწოდოთ მომხმარებელს ვებგვერდზე რეგისტრაციისას „პერსონალური მონაცემების დამუშავების პოლიტიკის“ სახით დეტალური ინფორმაცია თუ რა მონაცემები და რა მიზნით უნდა დაამუშაოთ.

დაუშვებელია

მიაწოდოთ მომხმარებელს „კონფიდენციალურობის პოლიტიკით“ არასრული, არაზუსტი ინფორმაცია მათი პერსონალური მონაცემების დამუშავების შესახებ. მაგალითად, აცნობოთ, რომ ამუშავებთ მომხმარებლის ვებგვერდზე აქტივობების ისტორიის შესახებ ინფორმაციას, მაშინ, როდესაც აღნიშნული პერსონალური მონაცემი არ მუშავდება.

დაუშვებელია

გაუზიაროთ მომხმარებლის თანხმობის გარეშე მესამე პირებს მისი პერსონალური მონაცემები, გარდა კანონმდებლობით განსაზღვრული შემთხვევებისა.

4.4. მომხმარებლის თანხმობა

ონლაინ ვაჭრობისას უნდა დარწმუნდეთ, რომ მომხმარებელმა, რომლის შესახებ პერსონალური მონაცემიც მუშავდება წინასწარ, თავისი ნებით ნათლად გამოთქვა თანხმობა პერსონალურ მონაცემთა დამუშავებაზე და მას ჰქონდა მიღებული დამუშავების მიზნის შესახებ სრული ინფორმაცია.

აუცილებელია, რომ თანხმობა იყოს:

- ნებაყოფლობითი.
- გამოხატული წინასწარ, პერსონალურ მონაცემთა დამუშავებამდე.
- გამოხატული პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის მიღების შემდეგ.
- გამოხატული კონკრეტული, მკაფიოდ განსაზღვრული კანონიერი მიზნით მონაცემთა დამუშავებაზე.
- გამოხატული ისეთი საშუალებით, რომლითაც ნათლად დგინდება მომხმარებლის ნება.

მნიშვნელოვანია

დარწმუნდეთ, რომ მომხმარებლის პერსონალურ მონაცემთა დამუშავებამდე სახეზეა თანხმობის კანონიერებისთვის განსაზღვრული ყველა ზემოაღნიშნული კომპონენტი.

მნიშვნელოვანია

გაითვალისწინოთ, რომ მომხმარებლის თანხმობა არ ნიშნავს, რომ ნებისმიერი მიზნით შეგიძლიათ დაამუშაოთ მისი პერსონალური მონაცემები. მიუხედავად თანხმობისა, უნდა დაიცვათ ყველა პრინციპი, რომელიც ჩამოთვლილია წინამდებარე რეკომენდაციების ქვეთავში - ძირითადი წესები.

5. პერსონალურ მონაცემთა პირდაპირი მარკეტინგის მიზნებისთვის დამუშავება

სავაჭრო ორგანიზაციები ხშირად მომხმარებლებს თავიანთი პროდუქტის, ან შეთავაზების შესახებ ატყობინებენ პირდაპირი მარკეტინგის გზით.

პირდაპირი მარკეტინგი გულისხმობს მომხმარებლისთვის მოკლე ტექსტური შეტყობინების, სატელეფონო ზარის, ელექტრონული ფოსტის საშუალებით საქონლის, მომსახურების ან დასაქმების შეთავაზებას.

ონლაინ ვაჭრობისას მომხმარებელთა პერსონალური მონაცემები პირდაპირი მარკეტინგის მიზნებისთვის შეგიძლიათ შეაგროვოთ:

- საჯაროდ ხელმისაწვდომი წყაროებიდან, ან
- უშუალოდ მომხმარებლისგან.

საჯაროდ ხელმისაწვდომი წყაროებიდან შეგიძლიათ შეაგროვოთ მომხმარებელთა მხოლოდ შემდეგი პერსონალური მონაცემები:

- სახელი და გვარი.
- მისამართი.
- ტელეფონის ნომერი.
- ელ-ფოსტა.
- ფაქსის მისამართი.

იმ შემთხვევაში თუ მომხმარებლის შესახებ გროვდება სხვა სახის პერსონალური მონაცემები აუცილებელია მომხმარებლის წერილობითი თანხმობა.

მნიშვნელოვანია

გაითვალისწინოთ, რომ თქვენ ხართ პასუხისმგებელი პირდაპირი მარკეტინგის მიზნებისთვის პერსონალურ მონაცემთა დამუშავებაზე, მიუხედავად იმისა, უშუალოდ ახორციელებთ მარკეტინგს თუ, მაგალითად სარეკლამო კომპანიის მეშვეობით.

დაუშვებელია

გამოიყენოთ კანონმდებლობის მოთხოვნათა დარღვევით გასაჯაროებული პერსონალური მონაცემები პირდაპირი მარკეტინგის მიზნებისათვის.

მნიშვნელოვანია

დარწმუნდეთ, რომ ინფორმაცია გასაჯაროებულია კანონიერად - უშუალოდ მომხმარებლის მიერ, მისი თანხმობით ან იმ შემთხვევაში, როდესაც ცალკეული მონაცემების საჯაროობა განსაზღვრულია კანონმდებლობით.

მნიშვნელოვანია

შეწყვიტოთ პირდაპირი მარკეტინგის მიზნებისთვის მომხმარებლის პერსონალური მონაცემების დამუშავება იმ შემთხვევაშიც, თუ მან გამოიყენა შეთავაზებულისგან განსხვავებული უარის თქმის მექანიზმი. მაგალითად, მომხმარებელმა მოკლე ტექსტურ შეტყობინების გამოგზავნის ნაცვლად, ელექტრონული ფოსტით გამოხატა უარი თავისი პერსონალური მონაცემების დამუშავებაზე.

მნიშვნელოვანია

დაურთოთ თითოეულ გაგზავნილ შეტყობინებას უარის თქმის მექანიზმი და მკაფიო მითითება იმაზე, თუ როგორ შეუძლია მომხმარებელს სარეკლამო შეტყობინების მიღების შეწყვეტა.

საუკეთესო პრაქტიკის გათვალისწინებით, სასურველია, აამოქმედოთ წინასწარი არჩევანის (opt in) მიდგომა და იმ შემთხვევაში გაუგზავნოთ მომხმარებელს შეტყობინებები, თუ მან ამის სურვილი გამოთქვა.

მომხმარებლებს უფლება აქვთ, ნებისმიერ დროს მოგთხოვონ თავიანთი პერსონალური მონაცემების პირდაპირი მარკეტინგის მიზნებისთვის გამოყენების შეწყვეტა იმავე ფორმით, რა ფორმითაც განხორციელდა მარკეტინგი.

ვალდებული ხართ მოთხოვნის მიღებიდან 10 სამუშაო დღეში შეწყვიტოთ პირდაპირი მარკეტინგის მიზნებისთვის მომხმარებლის პერსონალური მონაცემების გამოყენება.

6. პერსონალურ მონაცემთა დამუშავება უფლებამოსილი პირის მეშვეობით

ონლაინ ვაჭრობისას შესაძლებელია ფიზიკური ან/და იურიდიული პირის მომსახურებით სარგებლობა. მაგალითად, შესაძლებელია დაიქირაოთ კომპანია ონლაინ ვაჭრობისას საჭირო ელექტრონული პროგრამების დაინსტალირებისა და გამართული მუშაობის უზრუნველსაყოფად, ან საკურიერო მომსახურების უზრუნველსაყოფად. თუ აღნიშნული კომპანია რაიმე ფორმით დაამუშავებს მომხმარებელთა პერსონალურ მონაცემებს თქვენთვის ან თქვენი სახელით, ის ჩაითვლება უფლებამოსილ პირად.

უფლებამოსილი პირის მიერ ონლაინ ვაჭრობისას პერსონალურ მონაცემთა დასამუშავებლად მასთან უნდა დადოთ წერილობითი ხელშეკრულება ან/და შესაბამისი სამართლებრივი აქტის საფუძველზე უნდა იყოს გათვალისწინებული პერსონალურ მონაცემთა დამუშავება (მაგალითად, კანონი, მინისტრის ბრძანება).

უფლებამოსილ პირთან გასაფორმებელ ხელშეკრულებაში უნდა გაითვალისწინოთ შემდეგი პუნქტები:

- შეთანხმების საგანი.
- პერსონალურ მონაცემთა დამუშავების ხანგრძლივობა.
- პერსონალურ მონაცემთა დამუშავების მიზანი.
- პერსონალური მონაცემების სახე.
- თქვენი და უფლებამოსილი პირის უფლებები და ვალდებულებები.
- კონფიდენციალურობის ვალდებულება.
- უსაფრთხოების სათანადო ზომები.
- ქვეკონტრაქტორების გამოყენების პირობები (ასეთის არსებობისას).
- მომხმარებლის უფლებები.
- ხელშეკრულების გაუქმების პირობები და სხვ.

დაუშვებელია

უფლებამოსილი პირის მიერ, თქვენი თანხმობის გარეშე, მონაცემთა დამუშავების უფლების სხვა პირისთვის გადაცემა.

მნიშვნელოვანია

გაუწიოთ რეგულარული მონიტორინგი უფლებამოსილი პირის მიერ მომხმარებელთა პერსონალური მონაცემების დამუშავებას ონლაინ ვაჭრობისას.

დაუშვებელია

დადოთ ხელშეკრულება უფლებამოსილ პირთან, თუ არსებობს მის მიერ ონლაინ ვაჭრობისას მომხმარებელთა პერსონალური მონაცემების არამიზნობრივი დამუშავების საფრთხე.

დაუშვებელია

უფლებამოსილი პირის მიერ დამუშავდეს მომხმარებელთა პერსონალური მონაცემები ხელშეკრულებით ან/და სამართლებრივი აქტით დადგენილისგან განსხვავებული მიზნით.

7. ონლაინ ვაჭრობისას მომხმარებლის უფლებები და მათი რეალიზაციის მექანიზმები

ონლაინ ვაჭრობისას მომხმარებელს უფლება აქვს, მოგთხოვოთ:

- ინფორმაცია თუ რა პერსონალურ მონაცემებს ფლობთ ონლაინ ვაჭრობისას მის შესახებ.
- ინფორმაცია საიდან, რა მიზნითა და საფუძვლით მოიპოვეთ ონლაინ ვაჭრობისას მისი პერსონალური მონაცემები.
- ინფორმაცია იმის შესახებ, გაეცით თუ არა ონლაინ ვაჭრობისას მისი პერსონალური მონაცემები სხვა პირებზე.
- ონლაინ ვაჭრობისას არაზუსტი ან არასრული პერსონალური მონაცემების გასწორება, განახლება, დამატება და უსაფუძვლოდ შეგროვებული პერსონალური მონაცემების წაშლა, დაბლოკვა ან განადგურება.
- თანხმობის გამოხმობა ონლაინ ვაჭრობისას მისი პერსონალური მონაცემების დამუშავებაზე.

თქვენ ვალდებული ხართ:

- მოთხოვნის შემთხვევაში მიაწოდოთ ინფორმაცია მომხმარებელს ონლაინ ვაჭრობისას მის შესახებ რა პერსონალურ მონაცემებს, რა წყაროდან, რა მიზნითა და საფუძვლით ფლობთ.
- მოთხოვნის შემთხვევაში მიაწოდოთ ინფორმაცია მომხმარებელს ონლაინ ვაჭრობისას გაცემულა თუ არა მისი პერსონალური მონაცემები სხვა პირებზე და რა მიზნით.
- ინფორმაციის მიწოდების ფორმას ირჩევს მომხმარებელი, რაც იმას ნიშნავს, რომ მან შესაძლოა მოგთხოვოთ მონაცემებზე ინფორმაციის ელექტრონულად ან მატერიალურად გადაცემა. მას უფლება აქვს, მიიღოს მონაცემთა ასლები უსასყიდლოდ, გარდა იმ მონაცემებისა, რომელთა გაცემისთვის კანონმდებლობით დადგენილია გარკვეული საფასური.
- გასცეთ ინფორმაცია მოთხოვნისთანავე დაუყოვნებლივ, ან არაუგვიანეს 10 დღისა თუ პასუხის გაცემა მოითხოვს:
  - ინფორმაციის სხვა დაწესებულებაში ან სტრუქტურულ ერთეულში მოძიებასა და დამუშავებას ან მასთან კონსულტაციას.
  - მნიშვნელოვანი მოცულობის, ერთმანეთთან დაუკავშირებელი დოკუმენტების მოძიებასა და დამუშავებას.
  - სხვა დასახლებულ პუნქტში არსებულ სტრუქტურულ ქვედანაყოფთან ან სხვა საჯარო დაწესებულებასთან კონსულტაციას.
- გაასწოროთ, განაახლოთ, დაამატოთ, დაბლოკოთ, წაშალოთ ან გაანადგუროთ მომხმარებლის პერსონალური მონაცემები მოთხოვნის მიღებიდან 15 დღის ვადაში ან აცნობოთ მომხმარებელს უარის თქმის საფუძველი.
- აღრიცხოთ ონლაინ ვაჭრობისას მომხმარებლის პერსონალური მონაცემების მესამე პირებზე გაცემის შემთხვევები და აღნიშნული ინფორმაცია შეინახოთ გაცემულ პერსონალურ მონაცემებთან ერთად, მათი შენახვის ვადით.

8. უსაფრთხოების დაცვა

რეკომენდაციების ამ ნაწილის მიზანია, დაგეხმაროთ ინფორმაციული სისტემების განვითარების პროცესში:

- გააუმჯობესოთ ანგარიშვალდებულება მონაცემთა დაცვის კუთხით.
- მოაწყოთ IT პროცესების მართვასთან დაკავშირებული შიდა კონტროლის სისტემა და უზრუნველყოთ პერსონალურ მონაცემთა დაცვის საკანონმდებლო მოთხოვნებთან შესაბამისობა.

რეკომენდაციებში მოცემული საკითხები არ ფარავს IT სისტემების განვითარების ტექნიკურ მახასიათებლებს სრულად ან გამოსაყენებელ სპეციფიკურ ტექნოლოგიებს.

რეკომენდაციებში მოცემული ინფორმაცია შეიძლება გამოიყენოს სავაჭრო ორგანიზაციაში პერსონალურ მონაცემთა დაცვაზე პასუხისმგებელმა პირმა (მაგ: პერსონალურ მონაცემთა დაცვის ოფიცერი), ინფორმაციული ტექნოლოგიების თანამშრომელმა, რომელიც პასუხისმგებელია IT სისტემების მართვაზე და ყველა იმ პირმა, რომელიც უშუალოდ ეხება პერსონალურ მონაცემთა დამუშავების პროცესს.

რეკომენდაციები მომზადებულია ევროპის პერსონალურ მონაცემთა დაცვის საზედამხედველო ორგანოს[2] მიერ გამოცემული სახელმძღვანელოს გათვალისწინებით.[3]

8.1. ორგანიზაციების ანგარიშვალდებულება

ეფექტიანი შიდა კონტროლის სისტემის შექმნაზე პასუხისმგებელია სავაჭრო ორგანიზაცია, რომელმაც რეკომენდებულია ანგარიშვალდებულების პრინციპის გათვალისწინებით უზრუნველყოს შესაბამისი პროცესების მოწყობა.

სავაჭრო ორგანიზაცია პერსონალურ მონაცემთა დაცვის პოლიტიკით შესასრულებელი პასუხისმგებლობების დელეგირებას ახდენს პასუხისმგებლობებისა და უფლებამოსილებების ნათლად განსაზღვრითა და გადანაწილებით. სასურველია, დადგენილი იყოს ორგანიზაციული სტრუქტურა და პროცედურები, რომლებიც საოპერაციო გუნდს უზრუნველყოფს პერსონალურ მონაცემთა დამმუშავებლის როლის შესასრულებლად საჭირო უფლებამოსილებითა და საშუალებებით.

სასურველია, სავაჭრო ორგანიზაციამ დანიშნოს პერსონალურ მონაცემთა დაცვაზე პასუხისმგებელი პირი (მაგ: მონაცემთა დაცვის ოფიცერი (DPO), მონაცემთა დაცვის კოორდინატორი (DPC)) და უზრუნველყოს ის პერსონალურ მონაცემთა დაცვის პოლიტიკის დასანერგად საჭირო მანდატით. საუკეთესო პრაქტიკის გათვალისწინებით, სავაჭრო ორგანიზაციის საქმიანობის შედეგად პერსონალურ მონაცემთა დაცვის კუთხით გამოვლენილი ადამიანის ძირითადი უფლებების შელახვის შემთხვევების შესახებ პერსონალურ მონაცემთა დაცვის ოფიცერმა პირდაპირი ანგარიშგება უნდა მოახდინოს სავაჭრო ორგანიზაციის შიგნით.

სავაჭრო ორგანიზაციაში არსებულ მონაცემთა დაცვის პოლიტიკებსა და პროცედურებს უმჯობესია, რომ იცნობდეს ორგანიზაციის ყველა თანამშრომელი, ეს შესაძლებელია სავალდებულო გაცნობითი ტრენინგებით, საინფორმაციო მასალების მიწოდებით და ცნობიერების ამაღლების პერიოდული კურსებით.

სავაჭრო ორგანიზაციაში რეკომენდებულია რეგულარულად მოწმდებოდეს და გადაიხედებოდეს მონაცემთა დაცვასთან დაკავშირებული პოლიტიკები, პროცედურები, ასევე პასუხისმგებლობები და ფუნქციები.

8.2. პერსონალურ მონაცემთა დაცვის მოთხოვნები IT სისტემის განვითარების პროცესში

ამ თავში განხილულია IT სისტემების განვითარების სასიცოცხლო ციკლში (SDLC[4]), პერსონალური მონაცემების დამუშავების საკითხები და მოცემულია პერსონალურ მონაცემთა დაცვის მოთხოვნების ეფექტურად აღსრულების რეკომენდაციები.

[2] European Data Protection Supervisor – EDPS

[3] EDPS Guidelines on the protection of personal data in IT governance and IT management of EU institutions, 23.03.2018

[4] SDLC – Systems Development Life Cycle.

8.2.1. ინიცირება

ინიცირების ეტაპზე ხდება პროექტის მასშტაბის განსაზღვრა, ზოგადი მოთხოვნების ორგანიზაციის შიგნით შეთანხმება. იმის გათვალისწინებით, მოხდება თუ არა IT სისტემის გამოყენებით პერსონალური მონაცემების დამუშავება ან შექმნა, ორგანიზაციამ სასურველია, განიხილოს პროექტში მონაცემთა დაცვაზე პასუხისმგებელი პირის (DPO, DPC) ჩართვა, რომელიც დაეხმარება გუნდს პერსონალური მონაცემების დაცვის მოთხოვნების გათვალისწინებაში.

თუ შესაძლებელია, წინასწარ უნდა მოხდეს დასამუშავებელი პერსონალური მონაცემების განსაზღვრა, დაკავშირებული რისკების შეფასება და საჭირო უსაფრთხოების მექანიზმების შემუშავება.

8.2.2. დაგეგმვა

მოთხოვნების შეგროვება

IT სისტემის სპეციფიკაციის განსაზღვრის ეტაპზე დაინტერესებული მხარეებისგან უნდა მოხდეს პერსონალურ მონაცემთა დაცვის მოთხოვნების შეგროვება და დოკუმენტირება. პერსონალურ მონაცემთა დაცვის საკითხები აისახება ფუნქციურ და არაფუნქციურ მოთხოვნებში. ფუნქციური მოთხოვნები ძირითადად მოიცავს შესაძლებლობებს, რომლებიც საჭიროა მომხმარებლის უფლებების უზრუნველსაყოფად, როგორიც არის წვდომის, პერსონალურ მონაცემთა გადაცემის, შესწორების, წაშლის უფლება, ასევე ფუნქციებს, რომლებიც უზრუნველყოფენ პერსონალურ მონაცემთა დამუშავების ვადების შემცირებას. არაფუნქციური მოთხოვნები მოიცავს პერსონალურ მონაცემთა მინიმიზაციისა და მიზნის შეზღუდვის პრინციპების ზედამხედველობას, რომლის გათვალისწინება საჭიროა სისტემაში პერსონალურ მონაცემთა სტრუქტურის მოწყობისას, ასევე უსაფრთხოებისა და აუდიტირების მექანიზმების შემუშავებისას.

დიზაინი

დიზაინის ეტაპზე ხდება სისტემის არქიტექტურის, ფუნქციონალისა და პერსონალური მონაცემების დამუშავებისთვის საჭირო უსაფრთხოების ზომების განსაზღვრა.

პერსონალურ მონაცემთა დაცვის ფუნქციური და არაფუნქციური მოთხოვნების განხილვასთან ერთად, სავაჭრო ორგანიზაციამ უნდა გაითვალისწინოს შერჩეული ტექნოლოგიის პერსონალურ მონაცემთა დაცვის მახასიათებლები. მაგალითად, განსაზღვრული მიზნის შესაბამისად უნდა შეიცვალოს სისტემის პირველადი კონფიგურაცია, რომელიც ითვალისწინებს მეტი ინფორმაციის შეგროვებას ან მომხმარებლებზე დეტალური ჩანაწერების გაკეთებას.

თუ პერსონალურ მონაცემთა დამუშავების მოცულობას განსაზღვრავს მომხმარებელი, სისტემის პირველადი პარამეტრები უნდა მოეწყოს შეზღუდული ოპერაციების დამუშავების პრინციპის გათვალისწინებით, რომ მომხმარებელს მიეცეს რეალური შესაძლებლობა თავად აირჩიოს ოპერაციების დამუშავების სასურველი მასშტაბი.

უნდა შეიმუშაოთ და დანერგოთ კონტროლის ისეთი მექანიზმები, რომლებიც უზრუნველყოფენ პერსონალურ მონაცემთა კონფიდენციალობასა და მთლიანობას. პერსონალური მონაცემების დამუშავებისას, IT სისტემაში ინტეგრირებული კონტროლებით ავტორიზებულ პირებს წვდომა უნდა მიენიჭოთ მხოლოდ იმ პერსონალურ მონაცემებზე, რომელთა დამუშავება აუცილებელია პირისთვის დაკისრებული მოვალეობის შესასრულებლად. წვდომის კონტროლები დაეხმარება

სავაჭრო ორგანიზაციას, მიზნის შეზღუდვის პრინციპის გათვალისწინებით დაამუშაოს პერსონალური მონაცემები და დაიცვას არაავტორიზებული წვდომისგან.

თუ IT სისტემით მუშავდება პერსონალური მონაცემები, მაღალი რისკის შესამცირებლად, უნდა გამოიყენოთ დაცვის დამატებითი საშუალებები, როგორიც არის, მაგალითად, შიფრაცია და ორდონიანი ავთენტიფიკაცია.

შიფრაცია

პერსონალური მონაცემები აქტიურად გადადის ქსელიდან ქსელში ან ლოკალური შენახვის მოწყობილობიდან ღრუბლოვან ინფრასტრუქტურაში. პერსონალური მონაცემების მიმოცვლა დამატებით რისკებს შეიცავს, რის გამოც მნიშვნელოვანია მაქსიმალურად იყოს დაცული უსაფრთხოების ზომები.

პერსონალური მონაცემების უსაფრთხოებისთვის მნიშვნელოვანია შიფრაცია, როგორც ინფორმაციის გადაცემის პროცესში (data at transit) ასევე, სისტემაში შენახვისას (data at rest). პერსონალური მონაცემების დასაცავად, სავაჭრო ორგანიზაციებს შეუძლიათ, დაშიფრონ პერსონალური მონაცემები გადაადგილებამდე, გამოიყენონ დაშიფრული კავშირები (HTTPS, SSL, TLS, FTPS და ა. შ.) და შემნახველი მოწყობილობები.

ვებგვერდის ავთენტიფიკაციისა და პერსონალურ მონაცემთა დაცვის მიზნით რეკომენდებულია უსაფრთხოების პროტოკოლების გამოყენება, როგორიცაა Secure Sockets Layer (SSL). SSL იცავს როგორც ორგანიზაციას, ასევე მომხმარებლებს და ხელს უშლის პოტენციურ თავდამსხმელებს ფინანსური ან სენსიტიური ინფორმაციის მოპოვებაში. SSL პროტოკოლის საშუალებით მონაცემების გადაცემის დროს შიფრაციის პროცესში უმჯობესია Extended Validation სერტიფიკატის (EV SSL) გამოყენება, რომელიც მომხმარებლებს დაარწმუნებს ვებგვერდის მფლობელის ავთენტურობაში.

შეჯამება და საუკეთესო პრაქტიკა:

- დარწმუნდით, რომ პერსონალური მონაცემებისა და ზოგადად მონაცემების გადაცემა ხდება SSL/TLS პროტოკოლის გამოყენებით;
- შეამოწმეთ, რომ ყველა SSL და TLS სერვისი იყენებს ვალიდურ სერტიფიკატს და ვადის გასვლის შემთხვევაში, განაახლეთ სერტიფიკატები;
- SSL პროტოკოლის გამოყენების დროს რეკომენდებულია Extended Validation სერტიფიკატის (EV SSL) გამოყენება.

ორდონიანი ავთენტიფიკაცია

ორდონიანი ავთენტიფიკაცია (2FA) წარმოადგენს უსაფრთხოების დამატებით კომპონენტს ავტორიზაციის პროცესში, რაც ართულებს პოტენციური თავდამსხმელებისთვის წვდომას პირის მოწყობილობებზე ან ონლაინ ანგარიშებზე. ორდონიანი ავთენტიფიკაციის დროს სისტემაში შესვლისას მომხმარებლის ID-სა და პაროლის გარდა სავალდებულოა დამატებითი ინფორმაცია, რომელიც შეიძლება იყოს:

- კუთვნილების ფაქტორი - ის, რაც მომხმარებელს გააჩნია, როგორიცაა პირადობის მოწმობის მონაცემები, მობილური ტელეფონის საშუალებით მიღებული დროებითი კოდები, მობილური მოწყობილობისა ან სმარტფონის აპლიკაციის საშუალებით გენერირებული კოდები და სხვა;
- ბიომეტრიული ფაქტორი - ის, რაც მომხმარებელს თანდაყოლილად გააჩნია, მაგ: თითის ანაბეჭდი, სახის გამოსახულების ანაბეჭდი, ხმის ან ვიზუალური ჟესტის ჩანაწერი და სხვა;
- მდებარეობის ფაქტორი - ლოკაციის შესახებ ინფორმაცია, საიდანაც ხდება ავტორიზაციის მცდელობა. ეს შეიძლება განხორციელდეს ავთენტიფიკაციის მცდელობების შეზღუდვით კონკრეტულ მოწყობილობებზე, კონკრეტულ ადგილას ან ავტორიზაციის მცდელობის გეოგრაფიული წყაროს კონტროლით.

რეკომენდებულია ორდონიანი ავთენტიფიკაციის გამოყენება უკვე არსებული და გამოცდილი მობილური აპლიკაციების მეშვეობით, მაგალითად ყველაზე პოპულარული აპლიკაცია ორდონიანი ავთენტიფიკაციისათვის არის Google Authenticator, რომელიც ხელმისაწვდომია iOS და Android ოპერაციული სისტემების მქონე სმარტფონებში.

პერსონალურ მონაცემთა შენახვის ვადების მართვისთვის, უნდა შეიმუშაოთ IT სისტემაში პერსონალური მონაცემების შენახვის ვადების დაცვის სათანადო მექანიზმები და შენახვის ვადის გასვლის შემდგომ პერსონალურ მონაცემებზე განახორციელოთ შესაბამისი მოქმედებები, როგორიც არის პერსონალური მონაცემების ანონიმიზაცია და ან/და წაშლა.

ანონიმიზაციის ტექნიკებით უსაფრთხოების დაცვა და ეფექტიანი პროცესის მოწყობა შესაძლებელია მხოლოდ იმ შემთხვევაში, თუ სისტემა მოწყობილია სათანადოდ - ანონიმიზაციის პროცესის მიზანი და კონტექსტი განსაზღვრულია ნათლად და პერსონალური მონაცემების დამუშავებისას ხდება მიზნობრივი ანონიმიზაცია. ამ პროცესში ოპტიმალური გადაწყვეტილება მიიღება სიტუაციურად სხვადასხვა ტექნიკების გამოყენებით.

რა არის ანონიმიზაცია?

ანონიმიზაციის მიზანია შეამციროს პირის იდენტიფიცირების ალბათობა ან იდენტიფიცირებადობის შესაძლებლობა მისაღებ დონემდე. ამისათვის, მნიშვნელოვანია ***იდენტიფიცირებადობის*** საკითხის შეფასება და გათვალისწინება.

იდენტიფიცირების ***მახასიათებლები*** ცალკეულად არ წარმოადგენს პირის იდენტიფიცირების კრიტერიუმს. ამ დროს გასათვალისწინებელია ***კონტექსტიც*** - მაგალითად, დაბადების წლით პირის იდენტიფიცირება შესაძლებელია მისი ოჯახის კონტექსტში განხილვისას, თუმცა შეუძლებელია სკოლის ფარგლებში მისი გამოვლენა.

ანონიმიზაციის პროცესის ეფექტიანობა ფასდება იდენტიფიცირებადობის შემცირების მაჩვენებლით. კარგი პრაქტიკით ამ პროცესში განიხილავენ 3 ძირითად ინდიკატორს:

- ***გარჩევადობა*** - შესაძლებლობა პერსონალურ მონაცემთა ბაზიდან შეირჩეს კონკრეტული პირი;
- ***დაკავშირებულობა*** - შესაძლებლობა რამდენიმე მონაცემის დაკავშირებით მოხდეს პირის იდენტიფიცირება;
- ***პრედიქცია*** - შესაძლებლობა სხვადასხვა ინფორმაციის გამოყენებით მოხდეს მაიდენტიფიცირებელი მახასიათებლების გამოვლენა.

დაკავშირებულობის ინდიკატორი მთავარი პარამეტრია პერსონალური მონაცემების ***ფსევდონიმიზაციის*** პროცესში, რომლის გაიგივებაც ხშირად ხდება ანონიმიზაციასთან. ფსევდონიმიზაცია არის მონაცემთა იმგვარი დამუშავება, როდესაც ***დამატებითი ინფორმაციის*** გამოყენების გარეშე შეუძლებელია პერსონალური მონაცემების დაკავშირება კონკრეტულ მომხმარებელთან და ეს დამატებითი ინფორმაცია შენახულია ცალკე; როგორც განმარტებიდან ჩანს ***დამატებითი ინფორმაციის გამოყენების შემთხვევაში*** შესაძლებელია პირის იდენტიფიცირება, რის გამოც ფსევდონიმიზაციის შედეგად მიღებული ინფორმაცია წარმოადგენს ისევ პერსონალურ მონაცემს. ანონიმიზაციის შემთხვევაში, მას შემდეგ რაც მოხდება პერსონალური მონაცემების ანონიმიზაცია, ის კარგავს იდენტიფიცირებადობის შესაძლებლობას და აღარ ექვემდებარება „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მოქმედების სფეროს. შედეგად, მისი გამოყენება მარტივდება.

პერსონალურ მონაცემთა ანონიმიზაციაზე გადაწყვეტილების მიღებისას შესაფასებელია იდენტიფიცირებადობის რისკი - რამდენად შესაძლებელია ტექნიკურად და სამართლებრივად პერსონალური მონაცემების იდენტიფიცირება გონივრული ალბათობისა და კონტექსტის გათვალისწინებით. შესაფასებლად დაგეხმარებათ შემდეგი კრიტერიუმები:

- რამდენად დიდ ხარჯებს უკავშირდება მისი იდენტიფიცირება - ადამიანური და ფინანსური ფაქტორები;
- იდენტიფიცირებისთვის საჭირო დრო;
- პერსონალურ მონაცემთა დამუშავების დროს არსებული ტექნოლოგიური გარემო;
- ტექნოლოგიის განვითარების ტენდენციები.

ამ პროცესში საყურადღებოა პერსონალური მონაცემების გაზიარების კონტექსტი, ინფორმაციის გამჟღავნება იგეგმება ორგანიზაციასთან, ორგანიზაციების ჯგუფთან თუ ფართო წრისთვის გასაჯაროება.

შეფასებული რისკის დონის შესაბამისად განსხვავებულია ანონიმიზაციის ტექნიკების შერჩევის მიდგომებიც.

3. განხორციელება

განხორციელების ეტაპზე იწერება კოდი და იმ შემთხვევაში, თუ სისტემა მოიცავს კომპიუტერულ მოწყობილობებსაც, ხდება მათი დიზაინისა და კონფიგურაციის გათვალისწინება შეფასებული რისკების საპასუხოდ.

მნიშვნელოვანია, დეველოპერებსა და დაინტერესებულ მხარეებს შორის ჩამოყალიბდეს საერთო ხედვა და მოხდეს შინაარსობრივი შეთანხმება. განხორციელების ეტაპის დაწყებამდე დეველოპერების გუნდი უნდა გაეცნოს პერსონალურ მონაცემთა დაცვის მარეგულირებელ კანონმდებლობას, რაც შეიძლება განხორციელდეს, მაგალითად, DPO-ს მიზნობრივი ტრენინგებით და დეველოპერების ჯგუფის გადამზადებით.

4. ტესტირება და დანერგვა

ტესტირების ეტაპით ხდება განსაზღვრა რამდენად აკმაყოფილებს IT სისტემა პროექტით გათვალისწინებულ ყველა მოთხოვნას.

ტესტირებისას და ტესტირების სცენარის შემუშავებისას გასათვალისწინებელია მონაცემთა დაცვის ყველა მოთხოვნა, მათ შორის, მონაცემთა დაცვაზე მკაფიო და ინფორმაციული შეტყობინების არსებობა, მონაცემთა ხარისხისა და მზა ჩანაწერების მართვის (cookies) ფუნქციონალის არსებობა, კონფიდენციალურობის დამხმარე პირველადი კონფიგურაცია და IT უსაფრთხოების მოთხოვნები.

მონაცემთა დაცვის მოთხოვნებთან შესაბამისობის უზრუნველსაყოფად მიზანშეწონილია, შეიმუშაოთ ტესტირების პროცედურები და ინსტრუქციები, პერსონალური მონაცემები დაამუშაოთ მინიმიზაციის პრინციპის გათვალისწინებით და განსაზღვროთ უსაფრთხოების დამატებითი ტექნიკური და ორგანიზაციული ზომები სატესტო გარემოსთვის.

ტესტირების ეტაპზე არ არის მიზანშეწონილი ავთენტური პერსონალური მონაცემების გამოყენება, რადგან:

- მონაცემები არ შეიძლება დამუშავდეს მათი შეგროვებისას განსაზღვრული მიზნისგან განსხვავებით;
- სატესტო გარემოში პერსონალური მონაცემები შეიძლება ხელმისაწვდომი გახდეს არაავტორიზებული პირებისთვის.

სადაც შესაძლებელია, უნდა გამოიყენოთ ხელოვნურად შექმნილი სატესტო მონაცემები (მაგ: სიმულაციური ბაზები), ან თუ ავთენტური მონაცემების გამოყენების გარეშე ტესტირებით ვერ მიიღება სისტემის ვალიდურობის შესახებ საკმარისი შეფასება, უნდა მოხდეს გადაწყვეტილების დასაბუთება და შესაბამისად დოკუმენტირება. ავთენტური პერსონალური მონაცემების გამოყენების შემთხვევაში მიზანშეწონილია მათი ანონიმიზაცია.

ტესტირების ეტაპის შემდგომ ხდება სისტემის გადატანა რეალურ გარემოში და მომხმარებლებისა და სისტემის მხარდამჭერი სპეციალისტების ცნობიერების ამაღლება.

8.2.3. ოპერაციები და მხარდაჭერა

საოპერაციო გარემო არის ყოველდღიური სამუშაო პროცესი, რომელიც მიმდინარეობს უწყვეტად და მეორდება განსაზღვრული ინტერვალით (მაგ: სარეზერვო ასლები, სისტემური განახლებები და სხვა).

ოპერაციები უნდა იმართებოდეს სისტემის განახლებული დოკუმენტებით, რომელიც ითვალისწინებს პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებულ სპეციფიკურ მოთხოვნებს.

ცვლილებების ან ახალი სერვისების დამატების შემთხვევაში უნდა გადაიხედოს და განახლდეს სისტემის საოპერაციო რისკები და კონფიდენციალობის პოლიტიკა.

უნდა განსაზღვროთ პერსონალურ მონაცემთა შენახვის მაქსიმალური ვადა მათი გამოყენებისა და მიზნობრიობის გათვალისწინებით.

8.2.4. მომხმარებლების ინფორმირება და გამჭვირვალობა

სასურველია, შეიმუშაოთ კონფიდენციალურობის პოლიტიკა და მოახდინოთ მისი კომუნიკაცია მომხმარებლებთან.

სათანადო საინფორმაციო ინსტრუმენტების შექმნა დამოკიდებულია IT სისტემების მახასიათებლებზე და მომხმარებლებთან კომუნიკაციის ფორმებზე. თუ სისტემა პერსონალურ მონაცემთა დამუშავების პროცესში პირდაპირ ხელმისაწვდომია სუბიექტებისთვის (მაგ: შიდა მართვის სისტემა თანამშრომლებისთვის), მას უნდა ჰქონდეს პერსონალურ მონაცემთა დამუშავების შესახებ ინფორმირების შესაბამისი ფუნქციონალი მომხმარებლისთვის.

თუ მომხმარებელს არ აქვს პირდაპირი წვდომა სისტემაზე, ინფორმაცია დამუშავების შესახებ შესაფერის დროს უნდა მიეწოდოს მომხმარებელს (მაგ: როცა პერსონალური მონაცემების შეგროვება ხდება აპლიკაციის მეშვეობით, აპლიკაციაში უნდა მიეთითოს ამის შესახებ ინფორმაცია ან გაკეთდეს ბმული ინფორმაციის წყაროზე).

მომხმარებლის მიერ ინფორმაციის მოთხოვნის შემთხვევაში სავაჭრო ორგანიზაციამ უნდა უზრუნველყოს ინფორმაციის მიწოდება (მაგალითად, შექმნას ზოგადი ელ-ფოსტა მსგავსი შეტყობინებების მისაღებად) და რეაგირება გონივრულ ვადაში.

8.2.5. წვდომის კონტროლები

უნდა განსაზღვროთ სისტემის მფლობელი და რისკების რეგულარულ მართვაზე პასუხისმგებელი პირი. სისტემის მფლობელმა უნდა უზრუნველყოს სისტემაზე წვდომის კონტროლები, სათანადოდ მართოს IT უსაფრთხოების ინციდენტები და დანერგოს სხვა კონტროლები, რომლებიც შესაბამის რისკებს ეხმიანება.

პირის პერსონალურ მონაცემებზე წვდომა უნდა განხორციელდეს მინიმალური პრივილეგიების პრინციპის დაცვით. მაგალითად, მომხმარებელს და ადმინისტრატორს მონაცემებზე წვდომა უნდა გააჩნდეთ მხოლოდ დაკისრებული ვალდებულებების შესასრულებლად.

სასურველია, რეგულარულად გადახედოთ პერსონალურ მონაცემებზე წვდომის პროცედურებს და შეაფასოთ მათი საოპერაციო ეფექტიანობა.

პაროლების ჰეშირება და პარამეტრები

სისტემაზე წვდომის მართვის პროცესში ძირითად კონტროლის მექანიზმს წარმოადგენს პაროლების ეფექტიანი მართვა, მათ შორის მათი ჰეშირება და კომპლექსურობა.

ჰეშირება წარმოადგენს პაროლების დაცულობის მთავარ საფუძველს. ჰეშირების მეთოდები

დროდადრო იცვლება და იხვეწება, ამიტომ, მნიშვნელოვანია გამოყენებული მეთოდების მუდმივი შეფასება და განახლება. მაგალითად, მეთოდი როგორიცაა SHA-1 ან MD5 არ არის აღიარებული ჰეშირების სანდო მექანიზმად აკრედიტირებული პროფესიული ინსტიტუტების მიერ (მაგ: NIST).

ჰეშირების მეთოდის შერჩევისას უნდა გამოიყენოთ პაროლების ჰეშირების სქემა (მაგ: PBKDF2, bcrypt, scrypt), რომელიც პოტენციური თავდამსხმელებისთვის მაქსიმალურად ზრდის პაროლების გამოცნობის დროს.

რაც შეეხება პაროლების კომპლექსურობას, რეკომენდებულია:

- პაროლი არ იყოს სიტყვა ან სახელი.
- არ შეიცავდეს მომხმარებლის სახელს, მისამართს ან დაბადების თარიღს.
- შედგებოდეს 8 ან მეტი სიმბოლოსგან.
- შეიცავდეს დიდ და პატარა ასოებს, ციფრებსა და სპეციალურ სიმბოლოებს, როგორებიცაა, მაგალითად, ‘*’, ‘/’, ‘&’.

პაროლების მართვის საუკეთესო პრაქტიკები

- არ შეინახოთ პაროლები ტექსტური ფორმატით, ან არადაშიფრული სახით;
- გამოიყენეთ პაროლების ჰეშირების ფუნქცია;
- პერიოდულად შეამოწმეთ ჰეშირების მეთოდის სიძლიერე;
- გამოიყენეთ რთული პაროლები;
- პაროლების გამყღავნების შემთხვევაში წინასწარ შეიმუშავეთ გეგმა, რომლის მიხედვითაც იმოქმედებთ;
- რისკების არსებობის შემთხვევაში, პროგრამაში მომხმარებლის სახელისა და პაროლის რამდენჯერმე არასწორი გამოყენების მცდელობის შემთხვევაში, შესაბამისი მომხმარებელი უნდა იბლოკებოდეს (სრულად თუ არა, გარკვეული დროით მაინც);
- საჭიროების შემთხვევაში, გამოიყენეთ ავტომატიზებული და ინტენსიური ავტორიზაციის მცდელობებისაგან დაცვის მექანიზმები (მაგ. CAPTCHA);
- თუ თქვენი პროგრამა ამუშავებს დიდი რაოდენობით კონფიდენციალურ მონაცემებს, ავთენტიფიკაციისათვის გამოიყენეთ არა მარტო მომხმარებლის სახელი და პაროლი, არამედ, ასევე ერთჯერადი დროებითი კოდები, რომლებიც მომხმარებელს შესაძლოა მიეწოდებოდეს მოკლე ტექსტური შეტყობინების, დამატებითი პროგრამების, ან მოწყობილობების საშუალებით;
- საჭიროების შემთხვევაში, სისტემაში აუცილებელი უნდა იყოს პაროლების პერიოდული ცვლილება;
- პაროლის ცვლილების დროს, შეუძლებელი უნდა იყოს არსებული/მანამდე რამდენიმე გამოყენებული პაროლის განმეორება. პაროლების ისტორიის რაოდენობა დამოკიდებული უნდა იყოს შესაბამისი რისკების ხარისხზე;
- პროგრამაში უნდა იყოს გათვალისწინებული მომხმარებლის მიერ პაროლის ცვლილების ფუნქციონალი, შესაბამისი ავტორიზაციისა და დადასტურების პროცედურით;
- პროგრამაში პაროლის ცვლილების დროს მომხმარებელთან უნდა მიდიოდეს შესაბამისი შეტყობინება, რათა შემცირდეს პაროლის არაავტორიზებული ცვლილებების ალბათობა;
- იმ შემთხვევაში, თუ პროგრამაში გათვალისწინებული იქნება ადმინისტრატორის მიერ პაროლის განულების (reset) ფუნქციონალი, მომხმარებელს უნდა ეგზავნებოდეს დროებითი პაროლი. დროებითი პაროლის გამოყენება შესაძლებელი უნდა იყოს მხოლოდ ერთჯერადად და შემდგომ, სავალდებულოდ უნდა მოითხოვდეს მომხმარებლის მიერ ახალი პაროლის შექმნას;
- პროგრამის ადმინისტრატორის პრივილეგიის მქონე მომხმარებლებისთვის პაროლების პოლიტიკა უნდა იყოს იმაზე უფრო მკაცრი, ვიდრე სტანდარტული მომხმარებლებისთვის. მაგალითად, თუ ჩვეულებრივი მომხმარებლისათვის დასაშვები იქნება მინიმუმ 8 სიმბოლოსგან შემდგარი კომპლექსური პაროლი, ადმინისტრატორისათვის პაროლის ზომის მინიმალური სიმბოლოების რაოდენობა უნდა იყოს 12 და ა. შ.;
- მომხმარებლის ნებისმიერი ავტორიზაციის მცდელობის შესახებ, ინფორმაცია მუდმივად შეინახეთ ჟურნალში, ე.წ. „ლოგების“ სახით.

8.2.6. უსაფრთხოების მართვა

მონაცემთა დაცვის მიზნით რეკომენდებულია, უზრუნველყოთ IT სისტემების დაცვა სათანადო უსაფრთხოების ტექნოლოგიებით, დანერგოთ უსაფრთხოების შეფასებისას

გამოვლენილი რისკების საპასუხო ზომები და მუდმივად განაახლოთ არსებული საფრთხეების შესაბამისად.

ინფორმაციული სისტემა უნდა იძლეოდეს აუდირებადი კვალის (ლოგების) გენერირების საშუალებას იმისათვის, რომ შესაძლებელი გახდეს სისტემაში განხორციელებული მოვლენებისა და ცვლილებების თანმიმდევრული აღდგენა.

მაგალითი: სისტემაში პროგრამული შეცდომის (bug) არსებობის შემთხვევაში მოერიდეთ რეალურ გარემოში კოდში ცვლილებას (debugging). ყველა შემთხვევაში, საჭიროების გათვალისწინებით, მოიპოვეთ პერსონალურ მონაცემთა დამმუშავებლის ავტორიზაცია ცვლილებაზე. დაადოკუმენტირეთ ცვლილებასთან დაკავშირებული ყველა ქმედება იმისათვის, რომ პროცესი გახდეს მიკვლევადი და აუდირებადი. ცვლილების ტესტირებისთვის გამოიყენეთ მინიმალური მონაცემები და შეზღუდეთ ე.წ. „Need to know“ პრინციპის გათვალისწინებით.

უნდა შეაფასოთ შეიცავს თუ არა უსაფრთხოების მონიტორინგის პროცესში შექმნილი ლოგები პერსონალურ მონაცემებს და განიხილოთ გამოვლენილი ფაქტები რისკების შეფასებისას. ამ პროცესშიც ნათლად უნდა განისაზღვროს პერსონალურ მონაცემთა დამუშავების მიზანი და შენახვის ვადა.

პროგრამული უზრუნველყოფის განახლება

ნებისმიერი პროგრამული უზრუნველყოფა დროთა განმავლობაში საჭიროებს განახლებას, რათა აღმოიფხვრას ის ნაკლოვანებები, რომლებიც მას მოწყვლადს ხდის პოტენციური თავდამსხმელებისთვის. ამისათვის, მნიშვნელოვანია განახლების გამოსვლისთანავე მათი ინსტალაცია და სატესტო გარემოში ტესტირება რეალურ გარემოში გადატანამდე.

რეკომენდებულია, როგორც უსაფრთხოების განახლების პოლიტიკის დანერგვა ორგანიზაციაში, ასევე პოლიტიკის შესაბამისად არსებული პროგრამული უზრუნველყოფის განახლება, რომელიც პერსონალური მონაცემების დასამუშავებლად გამოიყენება.

ელექტრონული კომერციის ინდუსტრიაში ხშირად კომპანიები პროდუქტს ყიდიან ვებგვერდით, რომლის ჰოსტინგსაც ახორციელებს მესამე მხარე. ამ დროს მნიშვნელოვანია, მათ შორის მკაცრად იყოს გამიჯნული და განსაზღვრული პასუხისმგებლობები, თუ ვინ რომელი კომპონენტის განახლებაზეა ანგარიშვალდებული.

ყურადღება უნდა გამახვილდეს მოწყობილობებზეც, რომლებსაც ეხებათ განახლებები. სავაჭრო ორგანიზაციამ უნდა გადაწყვიტოს რა მეთოდით განახორციელებს განახლებებს: მოწყობილობის განახლება ოფისს გარეთ მოხდება, ოფისს შიგნით თუ სხვა.

პროგრამულ უზრუნველყოფებზე განახლებები ძირითადად ავტომატურად ხორციელდება, შესაბამისად, საჭიროა მესამე მხარის მაღალი ნდობა. ამისათვის, სავაჭრო ორგანიზაციამ უნდა შეარჩიოს სანდო მომწოდებელი და განსაზღვროს ავტომატური განახლების პრაქტიკულობა.

შეჯამება და საუკეთესო პრაქტიკები

- რეკომენდებულია, შეიმუშაოთ პროგრამული უზრუნველყოფის განახლების პოლიტიკა ყველა პროგრამისთვის, რომელიც გამოიყენება პერსონალური მონაცემების დამუშავების პროცესში. პოლიტიკა უნდა ეხებოდეს ყველა რელევანტურ კომპონენტს, მათ შორის ოპერაციულ სისტემას, აპლიკაციებს, მონაცემთა ბაზას და ა.შ.;
- შეეცადეთ განახლების გამოსვლისთანავე განაახლოთ პროგრამები, თუ გადადების მიზეზი არ არსებობს;

- განსაზღვრეთ პასუხისმგებლობები სისტემის კომპონენტების განახლებაზე. ნებისმიერმა მხარემ უნდა იცოდეს რისი განახლება ევალება და რა პერიოდულობით.

8.2.7. პერსონალურ მონაცემთა გაცვლა

უნდა გამოავლინოთ პერსონალურ მონაცემთა მეორადი გამოყენების ან მესამე მხარესთან გაცვლის შემთხვევები, შეაფასოთ ამ პროცესებთან დაკავშირებული რისკები და დაგეგმოთ საპასუხო მოქმედებები.

მაგალითი: როდესაც პერსონალური მონაცემების გაცვლა ხდება ინტერნეტით, საჭიროა მათი დაცვა ქსელის გამოყენებასთან დაკავშირებული თანდაყოლილი საფრთხეების მიმართ.

შიფრაციის გამოყენების შემთხვევაში უნდა მოხდეს გამოყენებული ინსტრუმენტის კონფიგურაციის სათანადოდ მოწყობა გამოყენებული კრიპტოგრაფიული გასაღების სათანადო მართვასთან ერთად.

8.2.8. სისტემის ჩამოწერა

პროგრამული უზრუნველყოფისა და მოწყობილობების ჩამოწერისას ან მათი გადატანისას განსხვავებულ გარემოში, უნდა შეიმუშაოთ და დანერგოთ პროცედურები პერსონალური მონაცემების მოთხოვნების დასაცავად.

იმ შემთხვევაში, თუ IT სისტემა აღარ პასუხობს არსებულ ბიზნეს საჭიროებებს, აღარ გამოიყენება ან გადაეცემა სხვას, საჭიროა ყურადღება მიექცეს პერსონალურ მონაცემებს, რათა არ მოხდეს მათი გამჟღავნება.

IT სისტემის ჩამოწერისას დაცული უნდა იყოს პერსონალური მონაცემების შენახვის შეთანხმებული ვადა.

ძველ IT სისტემებზე, რომლებიც შეიცავს პერსონალურ მონაცემებს და სისტემაზე წვდომის საჭიროება არ არის ან ვერ ხერხდება დასაბუთება, უნდა შეიზღუდოს დაშვება.

უნდა შეიმუშაოთ პროცედურები და სამუშაო ინსტრუქციები პერსონალური მონაცემების შემცველი ელექტრონული ფაილების და მოწყობილობების (მაგ: შემნახველი მედია მატარებელი) განადგურებაზე.

8.2.9. შესყიდვა და აუთსორსინგი

IT სისტემის განვითარებისას სავაჭრო ორგანიზაცია ხშირად იღებს გადაწყვეტილებას სერვისის აუთსორსზე გატანის შესახებ. დადებითი გადაწყვეტილების შემთხვევაში, სავაჭრო ორგანიზაცია იწყებს შესყიდვის პროცედურებს.

მესამე მხარესთან გაფორმებული ხელშეკრულება უნდა მოიცავდეს უსაფრთხოების ტექნიკურ და ორგანიზაციულ მოთხოვნებს, რომლებმაც უნდა უზრუნველყონ პერსონალური მონაცემების დაცვა.

მონაცემების დაცვაზე პასუხისმგებელი პირი უნდა ჩაერთოს შესყიდვების პროცესში და ცოდნის გაზიარებით დაეხმაროს პროექტის ჯგუფს პერსონალური მონაცემების დაცვის მიმართულებით.

როგორც პერსონალურ მონაცემთა დამმუშავებელი, პასუხისმგებელი ხართ პროცესების კანონმდებლობის მოთხოვნებთან შესაბამისობაზე. აღნიშნულის გათვალისწინებით, უნდა უზრუნველყოთ ყველა რელევანტური რეკომენდაციის გათვალისწინება, მათ შორის მესამე

მხარის მიერ რეკომენდაციების სრულფასოვანი აღსრულება.

მიუხედავად იმისა, რომ დაგეგმვის პროცესში ორგანიზაციის მესამე მხარეების ვალდებულებები პირდაპირ არ არის განსაზღვრული, GDPR-ის მოთხოვნების ინტერპრეტაციისას ნათლად არის განმარტებული, რომ მათ პერსონალურ მონაცემთა დამმუშავებლის მსგავსად უნდა გაითვალისწინონ პერსონალური მონაცემების დაცვასთან დაკავშირებულ მოთხოვნები.

9. ონლაინ ვაჭრობისას პერსონალურ მონაცემთა კანონიერად დამუშავების დამხმარე საშუალებები

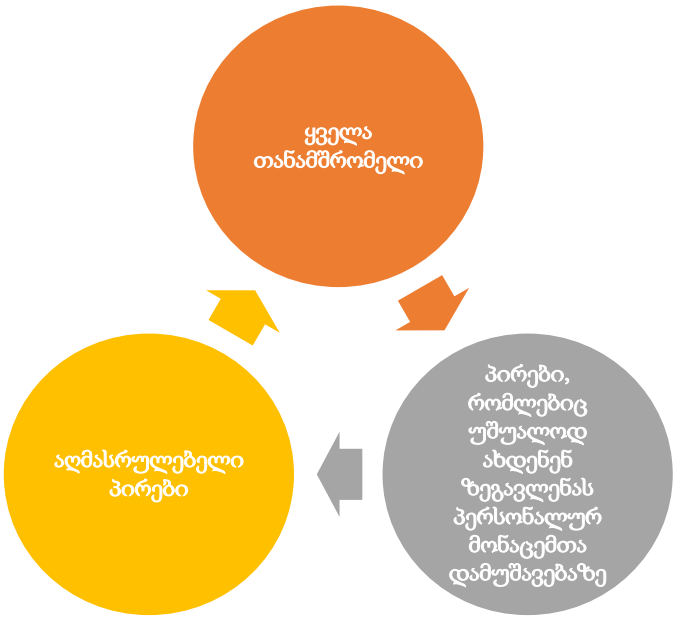
9.1. ცნობადობის ამაღლება

ონლაინ ვაჭრობისას სავაჭრო ორგანიზაციებში მომხმარებელთა პერსონალური მონაცემების დასაცავად და კანონიერად დამუშავებისთვის, რეკომენდებულია ყველა პირს, რომელიც ამ პერსონალურ მონაცემებს ამუშავებს, ჰქონდეს სათანადო ცოდნა:

- რა არის პერსონალური მონაცემი.
- რას ნიშნავს პერსონალურ მონაცემთა დამუშავება.
- რა ვალდებულებები აქვს პერსონალურ მონაცემთან შეხებისას.
- რა შემთხვევებშია დაშვებული პერსონალურ მონაცემთა გამოყენება.
- რა რისკებთანაა დაკავშირებული პერსონალურ მონაცემთა უკანონო დამუშავება.
- როგორ უნდა იმოქმედოს დარღვევების შემთხვევაში.

აღნიშნულ პირთა ინფორმირება უზრუნველყოფს პერსონალურ მონაცემთა დამუშავების კანონით დადგენილი მოთხოვნების დაცვას, რაც აგარიდებთ კანონით გათვალისწინებულ ადმინისტრაციულ პასუხისმგებლობებს.

რეკომენდებულია შესაბამისი პირების ინფორმირება მოახდინოთ საფეხურებად ტრენინგების, საინფორმაციო შეხვედრების მეშვეობით და დაყოთ აღნიშნული პირები შემდეგ რისკ-რგოლებად:



ყველა თანამშრომელი - უნდა იყოს ინფორმირებული თუ რა არის პერსონალური მონაცემი, რას ნიშნავს პერსონალურ მონაცემთა დამუშავება და რა მოვალეობები აქვს პერსონალურ მონაცემთა დამუშავებისას.

პირებს, რომლებიც უშუალოდ ახდენენ ზეგავლენას პერსონალურ მონაცემთა დამუშავებაზე - უნდა ჰქონდეთ შესაძლებლობა, გაუზიარონ პერსონალურ მონაცემთა დაცვასთან დაკავშირებით შეხედულებები სავაჭრო ორგანიზაციის მმართველ რგოლსა და აღმასრულებელ პირებს. აგრეთვე, ისინი უნდა იყვნენ ჩართული პერსონალური მონაცემების კანონიერად დამუშავების და პერსონალურ მონაცემთა დამუშავების პრინციპების დაცვის უზრუნველყოფაში. გარდა ამისა, აღნიშნული პირები უნდა იყვნენ ჩართული დისკუსიებში რისკების იდენტიფიკაციისა და შემცირების მიზნით.

აღმასრულებელი პირები - სავაჭრო ორგანიზაციების ხელმძღვანელ პოზიციებზე მყოფი პირები სათანადოდ უნდა იყვნენ ინფორმირებული პერსონალური მონაცემების დაცვის კანონმდებლობის მოთხოვნებისა და საერთაშორისო საუკეთესო პრაქტიკის შესახებ, რათა მათ შეძლონ დადასტურება, რომ სავაჭრო ორგანიზაციას პერსონალურ მონაცემთა დამუშავების კუთხით ყველაფერი შესაბამისობაში აქვს.

9.2. პერსონალური მონაცემების დაცვის პოლიტიკა ონლაინ სწავლებისას

რეკომენდებულია, გქონდეთ პერსონალური მონაცემების დამუშავების პოლიტიკა, რომელშიც გარდა მონაცემების დამუშავების მიზნებისა და საფუძვლებისა, განისაზღვრება პერსონალურ მონაცემთა დამუშავების ვადები, ელექტრონულ მონაცემებზე წვდომის წესები და პირობები და უსაფრთხოების გარანტიები. ასევე, აღნიშნული პოლიტიკით დადგინდება პერსონალურ მონაცემთა დამუშავებისას უფლებამოსილების ჯეროვანი განხორციელების მონიტორინგი და გამოვლენილ დარღვევებზე შესაბამისი რეაგირება. პოლიტიკა მომხმარებლებისთვის, ასევე, სავაჭრო ორგანიზაციის მონაცემთა დამუშავების პროცესებით დაინტერესებული სხვა პირებისთვის განკუთვნილი მნიშვნელოვანი დოკუმენტია და მონაცემების გამჭვირვალედ დამუშავებას მიანიშნებს.

9.3. პერსონალურ მონაცემთა დამუშავების ზეგავლენის შეფასება

სავაჭრო ორგანიზაციების მიერ პერსონალურ მონაცემთა დამუშავების ზეგავლენის შეფასება საუკეთესო პრაქტიკად ითვლება ბევრ ქვეყანაში. მიზანშეწონილია, დანერგოთ აღნიშნული პრაქტიკა ონლაინ ვაჭრობისას მაღალი რისკების მართვის მიზნით.

პერსონალურ მონაცემთა დამუშავების ზეგავლენის შეფასებისთვის შეგიძლიათ შექმნათ დოკუმენტი, რომელიც უნდა აღწერდეს პერსონალურ მონაცემთა კატეგორიას, მათი დამუშავების მიზნებს, პროპორციულობას, პროცესსა და საფუძვლებს, აფასებდეს ადამიანის ძირითადი უფლებების შელახვის შესაძლო საფრთხეებს და მონაცემთა უსაფრთხოების დაცვის მიზნით ითვალისწინებდეს გასატარებელ ზომებს.

აღნიშული პრაქტიკით სხვა სარგებლებთან ერთად, მოიპოვებთ შეჯიბრებით უპირატესობას კონკურენტ ორგანიზაციებთან მიმართებით.

9.4. პერსონალურ მონაცემთა დაცვის ოფიცერი

მიზანშეწონილია, დანიშნოთ ან განსაზღვროთ ონლაინ ვაჭრობისას პერსონალურ მონაცემთა დაცვის ოფიცერი, რომელიც იქნება პერსონალურ მონაცემთა დამუშავებაზე პასუხისმგებელი პირი.

პერსონალური მონაცემების დაცვის ოფიცერი:

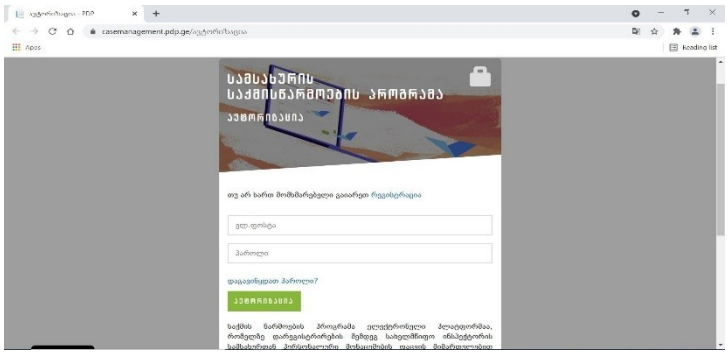
- მონიტორინგს გაუწევს პერსონალურ მონაცემთა დამუშავების პროცესში კანონმდებლობის მოთხოვნების შესრულებას.
- უზრუნველყოფს ორგანიზაციის ინფორმირებასა და კონსულტაციას პერსონალურ მონაცემთა დაცვის კანონმდებლობასა და მისი მოთხოვნების შესახებ.
- დაეხმარება ორგანიზაციას შეიმუშაოს პერსონალურ მონაცემთა დაცვის პოლიტიკა და პროცედურები.
- გააცნობს ორგანიზაციის თანამშრომლებს კანონმდებლობით და შიდა პოლიტიკებით დადგენილ ვალდებულებებს.
- უზრუნველყოფს პერსონალურ მონაცემთა დაცვის შესახებ ცნობიერების ამაღლებას, მათ შორის, მოამზადებს სატრენინგო კურსებს დასაქმებულთათვის და მომხმარებლებისთვის პერსონალურ მონაცემთა უსაფრთხოდ დამუშავების შესახებ.
- გასცემს კონსულტაციას და შეამოწმებს პერსონალურ მონაცემთა დამუშავების ზეგავლენის შეფასების პროცესს.
- იქნება მთავარი საკონტაქტო პირი სახელმწიფო ინსპექტორის აპარატთან და მომხმარებლებთან.

9.5. სახელმწიფო ინსპექტორის სამსახურთან კონსულტაცია

ონლაინ ვაჭრობისას პერსონალურ მონაცემთა დამუშავების სწორი პრაქტიკის დანერგვის მიზნით რეკომენდებულია, ნებისმიერ საკითხზე კონსულტაცია გაიაროთ სახელმწიფო ინსპექტორის სამსახურთან, რომლის ერთ-ერთ მთავარ ფუნქციას წარმოადგენს საქართველოში პერსონალურ მონაცემთა დამუშავების კანონიერების კონტროლი.

ამ მიზნით შესაძლებელია გამოყენებულ იქნას სახელმწიფო ინსპექტორის სამსახურის ვებგვერდზე არსებული საქმის წარმოების პროგრამა.

Casemanagement.pdp.ge



საქმის წარმოების პროგრამა ელექტრონული პლატფორმაა, რომელზე დარეგისტრირების შემდეგ სახელმწიფო ინსპექტორის სამსახურთან ნებისმიერი სახის კომუნიკაცია ერთ ონლაინ სივრცეშია შესაძლებელი. შეგიძლიათ მიიღოთ კონსულტაცია, გააგზავნოთ შეტყობინება, მიმართოთ სახელმწიფო ინსპექტორის სამსახურს განცხადებით და თვალი ადევნოთ რა ეტაპზეა თქვენი განცხადების თუ შეტყობინების განხილვა.

დანართი 1: მომხმარებლის თანხმობის ფორმა

ქვემოთ მოცემულია ონლაინ ვაჭრობისას მომხმარებლის პერსონალური მონაცემების დამუშავებაზე თანხმობის ნიმუში, რომელიც შესაძლებელია ადაპტირდეს თითოეული სავაჭრო ორგანიზაციის საჭიროებისა და სპეციფიკის შესაბამისად.

მე თანახმა ვარ, სასურველი პროდუქციის/მომსახურების მისაღებად დამუშავდეს სავაჭრო ორგანიზაციის ვებგვერდზე რეგისტრაციისას მითითებული ჩემი სახელი და გვარი, ელექტრონული ფოსტა და პაროლი.	კი ☐	არა ☐
მე თანახმა ვარ, სასურველი პროდუქციის/მომსახურების მიღების მიზნით დამუშავდეს სავაჭრო ორგანიზაციის ვებგვერდზე მითითებული ჩემი მისამართი.	კი ☐	არა ☐
მე თანახმა ვარ, სასურველი პროდუქციის/მომსახურების შესაძენად სავაჭრო ორგანიზაციის ვებგვერდზე შეკვეთის განთავსებისას ერთჯერადად დამუშავდეს ჩემი საბარათე მონაცემები.	კი ☐	არა ☐
მე თანახმა ვარ, სავაჭრო ორგანიზაციამ გამომიგზავნოს მარკეტინგული შეტყობინებები ახალ პროდუქციაზე/მომსახურებაზე, ფასდაკლებებზე ინფორმაციის მოწოდების მიზნით.	კი ☐	არა ☐
მე თანახმა ვარ, სავაჭრო ორგანიზაციამ გადასცეს საკურიერო კომპანიას ჩემი მისამართი და ტელეფონის ნომერი ჩემთვის შეკვეთის მოწოდების მიზნით.	კი ☐	არა ☐

დანართი 2: მზა ჩანაწერების ნიმუში

ქვემოთ მოცემულია მზა ჩანაწერების ნიმუში, რომელიც გამოიყენება ვებგვერდზე ვიზიტისას მომხმარებლებისთვის მზა ჩანაწერებთან დაკავშირებით ინფორმაციის მისაწოდებლად. აღნიშნული ნიმუში შესაძლებელია ადაპტირდეს თითოეული სავაჭრო ორგანიზაციის საჭიროებისა და სპეციფიკის შესაბამისად.

ჩვენ ვიყენებთ მზა ჩანაწერებს (Cookies), მომსახურების გასაუმჯობესებლად და თქვენთვის შესაბამისი რეკლამების მოწოდებისთვის.	ვეთანხმები ☐
მზა ჩანაწერების გამოყენების თაობაზე დამატებითი ინფორმაციის მისაღებად, გთხოვთ, გადახვიდეთ შემდეგ ბმულზე „მზა ჩანაწერების პოლიტიკა“.	არ ვეთანხმები ☐

ბმულზე გადასვლისას მომხმარებელს მიეწოდება შემდეგი ინფორმაცია:

მზა ჩანაწერების (Cookies) პოლიტიკა

მზა ჩანაწერები (Cookies) წარმოადგენს მცირე ზომის ტექსტურ ფაილებს, რომელსაც ვებგვერდი თქვენი სტუმრობისას თქვენსავე კომპიუტერში ან მობილურ ტელეფონში ინახავს. მზა ჩანაწერების მეშვეობით ჩვენ ვაკვირდებით ვებგვერდზე მომხმარებლების ქცევას, რათა მოვახდინოთ თქვენი გამოცდილების პერსონალიზება და მოგაწოდოთ შესაბამისი რეკლამები.

რა მზა ჩანაწერებს ვიყენებთ და როგორ?

ჩვენს ვებგვერდზე გამოიყენება შემდეგი მზა ჩანაწერები:

მზა ჩანაწერის დასახელება	ხანგრძლივობა (შენახვის ვადა)	აღწერა

დანართი 3: საკონტროლო სია

ქვემოთ მოცემულია პერსონალურ მონაცემთა დამუშავების საკონტროლო სია, რომელიც სავაჭრო ორგანიზაციებს დაეხმარებათ თვითშეფასებაში რამდენად არიან კანონმდებლობის მოთხოვნებთან შესაბამისობაში. იგი შემუშავდა GDPR-ის ოფიციალურ ვებგვერდზე განთავსებული სიის საფუძველზე.

სამართლებრივი საფუძველი და გამჭვირვალობა	
☐	ონლაინ ვაჭრობისას ფლობ ინფორმაციას თუ რა პერსონალურ მონაცემებს ამუშავებ და ვის აქვს წვდომა ასეთ პერსონალურ მონაცემებზე.
☐	ონლაინ ვაჭრობისას შეგიძლია სამართლებრივად დაასაბუთო თითოეული შენი მოქმედება პერსონალური მონაცემების მიმართ.
☐	შექმნილი გაქვს ონლაინ ვაჭრობისას პერსონალურ მონაცემთა დაცვის პოლიტიკა, რომელშიც ნათლადაა ასახული პერსონალურ მონაცემთა დამუშავებისას განხორციელებული მოქმედებები და მათი სამართლებრივი დასაბუთება.
პერსონალურ მონაცემთა უსაფრთხოება	
☐	ონლაინ ვაჭრობისას პერსონალურ მონაცემთა დაცვას იღებ მხედველობაში ნებისმიერი ახალი პროგრამის გამოყენებისას.
☐	როდესაც შესაძლებელია, ონლაინ ვაჭრობისას ახორციელებ პერსონალური მონაცემების შენახვას, ისე რომ მათი ამოცნობა შეუძლებელი იყოს.
☐	ონლაინ ვაჭრობისას ორგანიზაციაში დასაქმებულთათვის შექმნილი გაქვს უსაფრთხოების შიდა პოლიტიკა და ეწევი პერსონალურ მონაცემთა დაცვის კუთხით ცნობიერების ამაღლებას.
☐	იცი თუ რა დროს, როგორ და ვის მიმართო/შეატყობინო ონლაინ ვაჭრობის პროცესში პერსონალურ მონაცემთა დამუშავებისას გამოვლენილი დარღვევების თაობაზე.
ანგარიშვალდებულება	
☐	ორგანიზაციაში დანიშნული გყავს პერსონალურ მონაცემთა დამუშავებაზე პასუხისმგებელი პირი.
☐	ყველა მესამე პირთან, რომელიც შენი სახელით ამუშავებს პერსონალურ მონაცემებს ონლაინ ვაჭრობისას, გაქვს გაფორმებული ხელშეკრულება კანონით გათვალისწინებული ფორმით.
მომხმარებლის უფლებები	
☐	ონლაინ ვაჭრობისას მომხმარებლებს აწვდი სათანადო ინფორმაციას მათ შესახებ პერსონალურ მონაცემთა დამუშავების თაობაზე.

☐	მომხმარებლებს მარტივად შეუძლიათ, მოგმართონ ონლაინ ვაჭრობისას მათ შესახებ პერსონალურ მონაცემთა გასწორების, განახლების, დამატების, დაბლოკვის, წაშლის ან განადგურების მოთხოვნით
☐	დროულად აკმაყოფილებ მომხმარებლების თითოეულ მოთხოვნას ონლაინ ვაჭრობისას თავიანთი პერსონალური მონაცემების დამუშავების თაობაზე

დამატებით შეგიძლიათ გაეცნოთ სახელმწიფო ინსპექტორის სამსახურის ვებგვერდზე გამოქვეყნებულ თვითშეფასების კითხვარს.

რეკომენდაციები მომხმარებლებისთვის ონლაინ ვაჭრობისას პერსონალურ მონაცემთა დამუშავების თაობაზე

1. შესავალი

ახალი კორონავირუსით („COVID-19“) გამოწვეული პანდემიის პირობებში ციფრული ეკონომიკა და ონლაინ ვაჭრობა კიდევ უფრო განვითარდა. შესაბამისად, გაიზარდა ონლაინ ვაჭრობის პროცესში მომხმარებელთა პერსონალური მონაცემების დამუშავების რისკები.

მოცემული რეკომენდაციების მიზანია მომხმარებლებს მიეწოდოთ ინფორმაცია, როგორ უნდა დამუშავდეს მათი პერსონალური მონაცემები კანონიერად ონლაინ ვაჭრობისას და რა უფლებები აქვთ ამ კუთხით. აღნიშნული დაეხმარებათ, უკეთ გაიგონ რა გავლენა აქვს ონლაინ ვაჭრობას მათ პერსონალურ მონაცემებზე და რა ნაბიჯები შეუძლიათ გადადგან იმისთვის, რომ ჰქონდეთ უსაფრთხო ვირტუალური გარემო. შედეგად ისინი შეძლებენ, დაიცვან თავიანთი პერსონალური მონაცემები ონლაინ ვაჭრობისას და არ გახდნენ კანონდარღვევების მსხვერპლი.

რეკომენდაციები საინფორმაციო ხასიათისაა. მათ თან ახლავს მაგალითები, რომლებიც არ არის ამომწურავი და მოცემულია მხოლოდ საილუსტრაციოდ.

2. ტერმინთა განმარტება

2.1. პერსონალური მონაცემი

ნებისმიერი ინფორმაცია თქვენ შესახებ პერსონალური მონაცემია. მაგალითად:

- სახელი და გვარი.
- დაბადების თარიღი.
- პირადი ნომერი.
- ტელეფონის ნომერი.
- საცხოვრებელი მისამართი.
- ელექტრონული ფოსტის მისამართი.
- IP მისამართი.
- საბარათე მონაცემები.
- ვებგვერდზე სტუმრობის ფაქტი და გატარებული დრო.
- კომპიუტერული მოწყობილობის ტიპი.
- საოპერაციო სისტემა.
- ბრაუზერი.

2.2. პერსონალური მონაცემის დამუშავება

თქვენი პერსონალური მონაცემის მიმართ განხორციელებული ნებისმიერი მოქმედება პერსონალური მონაცემის დამუშავებაა. მაგალითად:

- ვებგვერდზე რეგისტრაციის მიზნით თქვენი ელექტრონული ფოსტის, პაროლის, სახელისა და გვარის მითითება.
- შეკვეთის განსანთავსებლად თქვენი საბარათე მონაცემების ასახვა.
- პროდუქციის/მომსახურების მოსაწოდებლად თქვენი საცხოვრებელი მისამართის გამოყენება.
- მარკეტინგული შეტყობინების გამოგზავნა თქვენს ტელეფონის ნომერზე ან ელექტრონულ ფოსტაზე.
- თქვენ მიერ ვებგვერდზე გატარებული დროის ნახვა.
- თქვენ მიერ ვებგვერდზე მოძიებული ინფორმაციის ნახვა.

3. ძირითადი წესები

პერსონალური მონაცემების დამუშავებისას მნიშვნელოვანია შემდეგი ოთხი გარემოება:

- პერსონალურ მონაცემთა დამუშავების საფუძველი (მაგალითად: მომხმარებლის თანხმობა).
- ონლაინ ვაჭრობისას მოთხოვნილი, შენახული, გამოყენებული, გაგზავნილი პერსონალური მონაცემების შესაბამისობა მონაცემთა დამუშავების პრინციპებთან (მაგალითად: ვადა, მიზანი).

- პერსონალურ მონაცემთა უსაფრთხოების უზრუნველყოფა, ანუ ის ორგანიზაციულ-ტექნიკური ზომები, რომლებიც მონაცემების შემთხვევითი და უკანონო გამჟღავნებისგან გიცავთ.

- მონაცემთა სუბიექტის უფლებების ხელმისაწვდომობა (მაგალითად: შესწორების, განახლების, შეცვლის, ინფორმირების და სხვა უფლებები).

საქართველოს კანონმდებლობა (მათ შორის, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი) ოთხივე საკითხს დეტალურად აწესრიგებს - ამომწურავად განსაზღვრავს საფუძვლებს, პრინციპებს, ადგენს ვადებს, უფლებების კონკრეტულ ჩამონათვალს და სხვა.

ონლაინ ვაჭრობის პროცესში სავაჭრო ორგანიზაციები ვალდებული არიან:

- დაამუშაონ თქვენი პერსონალური მონაცემები ონლაინ ვაჭრობისთვის საჭირო მოცულობით.
  - მაგალითად, დაამუშაონ თქვენი სახელი და გვარი ონლაინ შეკვეთის გასაფორმებლად.
- შეინახონ თქვენი ნამდვილი და ზუსტი პერსონალური მონაცემები.
  - მაგალითად, არ შეიყვანონ თქვენი მცდარი ელექტრონული ფოსტა მომხმარებელთა სიაში.
- განაახლონ თქვენი პერსონალური მონაცემები, რომლებიც შეიცვალა.
  - მაგალითად, ამ მიზნით მოგცენ საშუალება, განაახლოთ თქვენი პირადი ინფორმაცია (ტელეფონის ნომერი, მისამართი, ელექტრონული ფოსტა, პაროლი) ვებგვერდზე.
- შეინახონ თქვენი პერსონალური მონაცემები ონლაინ ვაჭრობისთვის საჭირო ვადით.
  - მაგალითად, ელექტრონული სისტემიდან წაშალონ თქვენი საბანკო ანგარიშის მონაცემები თქვენ მიერ შეკვეთის განთავსების შემდეგ.
- დაბლოკონ, წაშალონ ან გაანადგურონ თქვენი პერსონალური მონაცემები, რომლებიც აღარ სჭირდებათ ან შეინახონ ისეთი ფორმით, რომ თქვენი ამოცნობა შეუძლებელი იყოს.
  - მაგალითად, დაშიფრონ თქვენი პერსონალური მონაცემები - იდენტიფიცირებადი პირადი ინფორმაცია (მაგალითად, სახელი და გვარი) შეცვალონ ინიციალებით.
  - მაგალითად, მოგცენ საშუალება, სურვილის შემთხვევაში თავად წაშალოთ ვებგვერდიდან თქვენი პროფილი.

4. პერსონალურ მონაცემთა დამუშავების პროცესი ონლაინ ვაჭრობისას

4.1. ელექტრონულ პლატფორმებზე რეგისტრაცია/ავტორიზაცია/პროფილი/უკუკავშირი

სავაჭრო ორგანიზაციებში ონლაინ ვაჭრობის მიმდინარეობის პროცესი უმეტეს შემთხვევაში შემდეგია:

ვიზიტი ვებგვერდზე - მომხმარებელი სტუმრობს სავაჭრო ორგანიზაციის ვებგვერდს.

რეგისტრაცია - მომხმარებელი სასურველი პროდუქციის/მომსახურების შეძენის მიზნით რეგისტრირდება სავაჭრო ორგანიზაციის ვებგვერდზე და ავსებს შესაბამის ფორმას.

პროფილის შექმნა - რეგისტრაციისას საჭირო ფორმის შევსების შემდეგ იქმნება მომხმარებლის პროფილი.

მომსახურების/პროდუქციის შეძენა - მომხმარებელი ირჩევს სასურველ მომსახურებას/პროდუქციას და მათ შესაძენად დამატებით ავსებს თავის საბარათე მონაცემებს.

შეკვეთის მიწოდება - სავაჭრო ორგანიზაცია მომხმარებელს აწვდის სასურველ პროდუქციას/მომსახურებას. აღნიშნული შესაძლოა ასევე მოიაზრებდეს საკურიერო მომსახურების მეშვეობით მომხმარებლის მისამართზე პროდუქციის მიტანას.

უკუკავშირი - მომხმარებლებს შეუძლიათ ნებისმიერი კითხვის შემთხვევაში მიმართონ სავაჭრო ორგანიზაციას მათ ვებგვერდზე მითითებულ ნომერზე, ჩატში, ან ელექტრონულ ფოსტაზე.

4.2. ონლაინ ვაჭრობისას დამუშავებულ პერსონალურ მონაცემთა კატეგორიები

ონლაინ ვაჭრობის პროცესში სავაჭრო ორგანიზაციების მიერ ძირითადად მუშავდება მომხმარებელთა შემდეგი კატეგორიის მონაცემები: საიდენტიფიკაციო მონაცემები, საკონტაქტო ინფორმაცია, საბანკო მონაცემები, ვებგვერდზე განხორციელებული მოქმედებები.

საიდენტიფიკაციო მონაცემები - მომხმარებლები სავაჭრო ორგანიზაციის ვებგვერდზე რეგისტრაციისათვის უთითებენ საკუთარ სახელსა და გვარს, ასევე პროდუქციის შეძენის/მომსახურების მიღების მიზნით უთითებენ პირად ნომერს.

საკონტაქტო მონაცემები - მომხმარებლები სავაჭრო ორგანიზაციის ვებგვერდზე რეგისტრაციისათვის უთითებენ საკუთარ ელექტრონულ ფოსტასა და პაროლს, რომლითაც შეძლებენ ვებგვერდზე შესვლას და სასურველი პროდუქციის შეძენას/მომსახურების მიღებას. ამასთან, პროდუქციის/მომსახურების მისაღებად შეყავთ თავიანთი საცხოვრებელი ადგილის მისამართი და ტელეფონის ნომერი.

ვებგვერდზე განხორციელებული მოქმედებები - სავაჭრო ორგანიზაციები სხვადასხვა ელექტრონული პლატფორმის მეშვეობით აღრიცხავენ მომხმარებლების მიერ ვებგვერდზე განხორციელებულ მოქმედებებს, ასევე ვებგვერდზე სტუმრობის დროს, IP მისამართს, კომპიუტერული მოწყობილობის ტიპს, საოპერაციო სისტემასა და ბრაუზერს. აღნიშნული პერსონალური მონაცემების დამუშავება ხდება ე.წ. მზა ჩანაწერების (ე.წ. "Cookies") მეშვეობით. მზა ჩანაწერი ტექსტური ფაილია, რომელიც ავტომატურად იქმნება ვებგვერდზე ვიზიტის, მასზე არჩეული პარამეტრების, განთავსებული სარეგისტრაციო ინფორმაციის და ისტორიის (მაგალითად, ხშირად ნანახი პროდუქციის შესახებ) შესანახად. მზა ჩანაწერების საშუალებით ხდება მომხმარებლის მიერ მოძიებული ინფორმაციისა და ვებგვერდების დამახსოვრება, მომხმარებლის ქცევის და ინტერესების შესწავლა და აღნიშნულზე დაფუძნებით მისთვის სასურველი პროდუქტების/სერვისების ავტომატურ რეჟიმში შეთავაზება.

გარდა ზემოაღნიშნულისა, საყურადღებოა, რომ ონლაინ ვაჭრობისას ზოგიერთ პერსონალურ მონაცემზე მოქმედებს დაცვის უფრო მაღალი სტანდარტი. ასეთ პერსონალურ მონაცემებს კანონმდებლობა განსაკუთრებული კატეგორიის მონაცემებად მოიხსენიებს. მაგალითად:

- თქვენი ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცია.
- თქვენს ნასამართლობასთან, ადმინისტრაციულ პატიმრობასთან, საპროცესო გარიგებასთან დაკავშირებული ინფორმაცია.
- თქვენი რელიგიური შეხედულებები.
- თქვენი პოლიტიკური შეხედულებები.
- თქვენი სქესობრივი ცხოვრება.
- თქვენი ეთნიკური და რასობრივი კუთვნილების შესახებ ინფორმაცია.

განსაკუთრებული კატეგორიის მონაცემების დამუშავება სავაჭრო ორგანიზაციებს შეუძლიათ მხოლოდ გამონაკლის შემთხვევებში, მაგალითად, მომხმარებლის წერილობითი თანხმობით ან თუ ეს აუცილებელია მომხმარებლის სასიცოცხლო ინტერესების დაცვისთვის, და სხვ.

მნიშვნელოვანია	დაუშვებელია
გამოიჩინოთ მომეტებული ყურადღება ონლაინ ვაჭრობისას თქვენი განსაკუთრებული კატეგორიის პერსონალური მონაცემების დამუშავებისას.	სავაჭრო ორგანიზაციამ დაგავალდებულოთ მიაწოდოთ თქვენი ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცია.

5. პერსონალურ მონაცემთა პირდაპირი მარკეტინგის მიზნებისთვის დამუშავება

სავაჭრო ორგანიზაციები ხშირად თავიანთი პროდუქტის, ან შეთავაზების შესახებ მომხმარებლებს ატყობინებენ პირდაპირი მარკეტინგის გზით.

პირდაპირი მარკეტინგი გულისხმობს მომხმარებლებისთვის მოკლე ტექსტური შეტყობინების, სატელეფონო ზარის, ელექტრონული ფოსტის საშუალებით საქონლის, მომსახურების ან დასაქმების შეთავაზებას.

სავაჭრო ორგანიზაციებს ონლაინ ვაჭრობისას მომხმარებელთა პერსონალური მონაცემების პირდაპირი მარკეტინგის მიზნებისთვის შეუძლიათ შეაგროვონ:

- საჯაროდ ხელმისაწვდომი წყაროებიდან, ან
- უშუალოდ მომხმარებლისგან.

საჯაროდ ხელმისაწვდომი წყაროებიდან შესაძლებელია შეგროვდეს მომხმარებელთა მხოლოდ შემდეგი პერსონალური მონაცემები:

- სახელი და გვარი.
- მისამართი.
- ტელეფონის ნომერი.
- ელ-ფოსტა.
- ფაქსის მისამართი.

იმ შემთხვევაში თუ მომხმარებლის შესახებ გროვდება სხვა სახის პერსონალური მონაცემები აუცილებელია მომხმარებლის წერილობითი თანხმობა.

მნიშვნელოვანია	მნიშვნელოვანია
სავაჭრო ორგანიზაციამ შეწყვიტოს პირდაპირი მარკეტინგის მიზნებისთვის თქვენი პერსონალური მონაცემების დამუშავება იმ შემთხვევაშიც, თუ გამოიყენეთ შეთავაზებულისგან განსხვავებული უარის თქმის მექანიზმი. მაგალითად, მოკლე ტექსტურ შეტყობინების გაგზავნის ნაცვლად, ელექტრონული ფოსტით გამოხატეთ უარი თქვენი პერსონალური მონაცემების დამუშავებაზე.	იცოდეთ, რომ უფლება გაქვთ, ნებისმიერ დროს მოითხოვოთ თქვენი პერსონალური მონაცემების პირდაპირი მარკეტინგის მიზნებისთვის გამოყენების შეწყვეტა იმავე ფორმით, რა ფორმითაც განხორციელდა მარკეტინგი. სავაჭრო ორგანიზაცია ვალდებულია მოთხოვნის მიღებიდან 10 სამუშაო დღეში შეწყვიტოს პირდაპირი მარკეტინგის მიზნებისთვის თქვენი პერსონალური მონაცემების გამოყენება.

6. ონლაინ ვაჭრობისას მომხმარებლების უფლებები და მათი რეალიზაციის მექანიზმები

ონლაინ ვაჭრობისას უფლება გაქვთ, მოითხოვოთ:

- ინფორმაცია თუ რა პერსონალურ მონაცემებს ფლობს სავაჭრო ორგანიზაცია ონლაინ ვაჭრობისას თქვენ შესახებ.
- ინფორმაცია თუ საიდან, რა მიზნითა და საფუძვლით მოიპოვა ონლაინ ვაჭრობისას სავაჭრო ორგანიზაციამ თქვენი პერსონალური მონაცემები.
- ინფორმაცია, ხომ არ გაუცია სავაჭრო ორგანიზაციას ონლაინ ვაჭრობისას თქვენი პერსონალური მონაცემები სხვა პირებზე. ინფორმაციის მოწოდების ფორმას ირჩევთ თქვენ.
- პერსონალურ მონაცემთა ასლები უსასყიდლოდ, გარდა იმ პერსონალური მონაცემებისა, რომელთა გაცემისთვის კანონმდებლობით დადგენილია გარკვეული საფასური.
- ონლაინ ვაჭრობისას არაზუსტი ან არასრული პერსონალური მონაცემების გასწორება, განახლება, დამატება, და უსაფუძვლოდ შეგროვებული პერსონალური მონაცემების წაშლა, დაბლოკვა ან განადგურება.
- თანხმობის გამოხმობა ონლაინ ვაჭრობისას თქვენი პერსონალური მონაცემების დამუშავებაზე.

სავაჭრო ორგანიზაცია ვალდებულია:

- მოთხოვნის შემთხვევაში მოგაწოდოთ ინფორმაცია თუ რა პერსონალურ მონაცემებს ფლობს ონლაინ ვაჭრობისას თქვენ შესახებ, რა წყაროდან, რა მიზნითა და საფუძვლით. ასევე, გაცემულა თუ არა პერსონალური მონაცემები სხვა პირებზე და რა მიზნით.
- გასცეს ინფორმაცია მოთხოვნისთანავე დაუყოვნებლივ, ან არაუგვიანეს 10 დღისა.
- გაასწოროს, განაახლოს, დაამატოს, დაბლოკოს, წაშალოს ან გაანადგუროს თქვენი პერსონალური მონაცემები მოთხოვნის მიღებიდან 15 დღის ვადაში ან გაცნობოთ უარის თქმის საფუძველი.

მნიშვნელოვანია

გაეცნოთ დაწვრილებით ინფორმაციას ვებგვერდზე შესვლისთანავე მზა ჩანაწერების მეშვეობით პერსონალური მონაცემების დამუშავების შესახებ და მხოლოდ ამის შემდეგ დაეთანხმოთ მას.

მნიშვნელოვანია

დაინტერესდეთ, შეამოწმოთ და დაწვრილებით გაეცნოთ სავაჭრო ორგანიზაციის ვებგვერდზე განთავსებულ „პერსონალური მონაცემების დამუშავების პოლიტიკას“.

მნიშვნელოვანია

დაუკავშირდეთ სავაჭრო ორგანიზაციას, მაგალითად, ელექტრონული ფოსტის ან ტელეფონის ნომრის მეშვეობით, თქვენი პერსონალური მონაცემების დამუშავების შესახებ ნებისმიერ კითხვასთან დაკავშირებით.

7. ონლაინ ვაჭრობისას პერსონალურ მონაცემთა კანონიერად დამუშავების დამხმარე საშუალებები

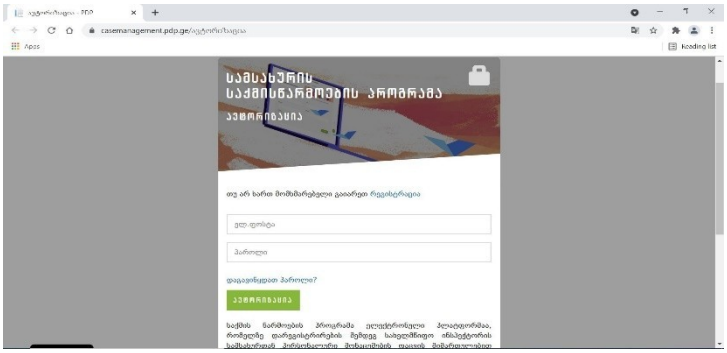
სახელმწიფო ინსპექტორის სამსახურთან კონსულტაცია

შეგიძლიათ ონლაინ ვაჭრობისას პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებით ნებისმიერ საკითხზე კონსულტაცია გაიაროთ სახელმწიფო ინსპექტორის სამსახურთან, რომლის ერთ-ერთ მთავარ ფუნქციას საქართველოში პერსონალურ მონაცემთა დამუშავების კანონიერების კონტროლი წარმოადგენს.

აგრეთვე, შეგიძლიათ სახელმწიფო ინსპექტორის სამსახურს მიმართოთ ონლაინ ვაჭრობისას პერსონალურ მონაცემთა დამუშავების დარღვევის ფაქტებთან დაკავშირებით.

ამ მიზნით შესაძლებელია გამოყენებულ იქნას სახელმწიფო ინსპექტორის სამსახურის ვებგვერდზე არსებული საქმის წარმოების პროგრამა.

Casemanagement.pdp.ge



საქმის წარმოების პროგრამა ელექტრონული პლატფორმაა, რომელზე დარეგისტრირების შემდეგ სახელმწიფო ინსპექტორის სამსახურთან ნებისმიერი სახის კომუნიკაცია ერთ ონლაინ სივრცეშია შესაძლებელი. შეგიძლიათ, მიიღოთ კონსულტაცია, გააგზავნოთ შეტყობინება, მიმართოთ სახელმწიფო ინსპექტორის სამსახურს განცხადებით და თვალი ადევნოთ რა ეტაპზეა თქვენი განცხადების თუ შეტყობინების განხილვა.

8. უსაფრთხოების დაცვა

8.1. შეამოწმეთ თქვენი მოწყობილობები

ონლაინ შესყიდვის განხორციელებამდე, პირველ რიგში, დარწმუნდით, რომ მოწყობილობა, რომელსაც შესყიდვისთვის იყენებთ არის განახლებული.

- დაიცავით თქვენი მოწყობილობები (ტელეფონი, კომპიუტერი, ტაბლეტი და სხვა) და მუდმივად განაახლეთ ოპერაციული სისტემა;
- ინტერნეტის მიმღები მოწყობილობის - firewall-ის (მარშუტიზატორის) ყიდვის შემდგომ, შეცვალეთ მოწყობილობის პირველადი (default) პაროლი და განაახლეთ რთული, კომპლექსური, ახალი პაროლით;
- შეამოწმეთ თქვენი მოწყობილობის კონფიდენციალობისა და უსაფრთხოების პარამეტრები, რომ იცნობდეთ როგორ ხდება ინფორმაციის გამოყენება, შენახვა და დარწმუნდით, რომ ინფორმაციის გაზიარება ხდება თქვენი არჩევანის შესაბამისად;
- სადაც შესაძლებელია, ჩართეთ ოპერაციული სისტემის ავტომატური განახლებები, იმისათვის, რომ ისარგებლოთ სისტემის უახლესი ვერსიით.

8.2. დაიცავით შესყიდვისთვის გამოყენებული ანგარიშის უსაფრთხოება

შეაფასეთ შესყიდვისთვის გამოყენებულ ანგარიშზე რამდენად იყენებთ ძლიერ პაროლს, ან სადაც შესაძლებელია, იყენებთ თუ არა მრავალფაქტორიან ავთენტიფიკაციას.

- სადაც შესაძლებელია, ერთჯერადი შესყიდვის შემთხვევაში, თუ არ გეგმავთ გახდეთ მუდმივი მომხმარებელი, მიზანშეწონილია არ შექმნათ შესყიდვის ვებგვერდზე ახალი ანგარიში (მაგალითად, Amazon.com-ზე 1-click ordering ფუნქციონალი);

- შესყიდვების ვებგვერდზე ახალი მომხმარებლის რეგისტრაციისას არ გამოიყენოთ თქვენს ძირითად ანგარიშებზე (მაგ: ელ-ფოსტა, სოციალური მედიის ანგარიშები, ონლაინ ბანკი, გადახდის პლატფორმის ანგარიში (PayPal, Google Pay, Apple Pay) გამოყენებული პაროლები. სხვადასხვა ანგარიშებზე იდენტური პაროლის გამოყენების შემთხვევაში მნიშვნელოვნად იზრდება ერთ-ერთ სავაჭრო პორტალზე პაროლის კომპრომეტირებით ყველა დანარჩენი ანგარიშის კომპრომეტირების რისკი. პერსონალურ მონაცემთა დარღვევების 80% ხდება მოპარული პაროლების სხვადასხვა პორტალებზე/საიტებზე გადასინჯვის მეთოდით;

- მიზანშეწონილია გამოიყენოთ ორდონიანი ავთენტიფიკაცია, რომელიც იდენტიფიცირების დასადასტურებლად იყენებს სხვადასხვა ინფორმაციას. იმ შემთხვევაშიც კი, თუ კიბერთაღლითები მოიპოვებენ თქვენს პაროლს, ისინი ვერ შეძლებენ ანგარიშზე წვდომას ორდონიანი ვერიფიკაციის გამო (მაგალითად, იმიტომ რომ არ აქვთ წვდომა თქვენს მობილურ ტელეფონზე, რომელზეც მოგდით ავთენტიფიკაციისთვის საჭირო ერთჯერადი კოდი).

როგორ უზრუნველვყო პაროლების უსაფრთხოება?

- გამოიყენეთ რთული პაროლი, რისთვისაც რეკომენდებულია:
  - პაროლი არ იყოს სიტყვა ან სახელი;
  - არ შეიცავდეს მომხმარებლის სახელს, მისამართს ან დაბადების თარიღს;
  - შედგებოდეს 8 ან მეტი სიმბოლოსგან;
  - შეიცავდეს დიდ და პატარა ასოებს, ციფრებსა და სპეციალურ სიმბოლოებს, როგორებიცაა, მაგალითად, ‘*’, ‘/’, ‘&’ და ა. შ.
- სადაც შესაძლებელია, გამოიყენეთ ორდონიანი ავთენტიფიკაციის მექანიზმი;
- პაროლები არ შეინახოთ ფიზიკური სახით, მაგ. ფურცელზე დაწერილი;
- თუ მოწყობილობას - კომპიუტერს, ტაბლეტს ან ლეპტოპს სხვა ადამიანიც იყენებს, პროგრამაში შესვლისას არ მონიშნოთ მომხმარებლის/პაროლის დამახსოვრების ველი. დარწმუნდით, რომ ანგარიშიდან გასვლის შემდეგ პაროლი შენახული არ არის;
- არ გაუზიაროთ თქვენი პაროლი სხვებს;
- შეეცადეთ არ გამოიყენოთ ერთი და იგივე პაროლი სხვადასხვა სისტემისთვის;
- შექმენით ინდივიდუალური პაროლი ყველა კრიკიტული სისტემისთვის;
- სასურველია, პერიოდულად განაახლოთ პაროლები.

შესყიდვისას ისარგებლეთ მხოლოდ სანდო ვებგვერდებით

ონლაინ სივრცეში ვაჭრობისას დაფიქრდით, როგორ ეძებთ პროდუქტს/მომსახურებას? ქსელთან დასაკავშირებლად იყენებთ სახლის თუ საჯარო ინტერნეტს? როგორ პოულობთ სასურველ ობიექტებს?

როგორც წესი, ფიზიკურად ვაჭრობის დროს მომხმარებლები არ სტუმრობენ მაღაზიას დასახელების გარეშე ან გაურკვეველი დასახელებით. იგივე წესები ვრცელდება ონლაინ ვაჭრობისას. თუ ვებგვერდი გამოიყურება საეჭვოდ, მაღალია რისკი, არ იყოს სანდო.

- პერსონალური თუ ფინანსური ინფორმაციის მიწოდებამდე, დარწმუნდით, რომ ურთიერთობთ სანდო მიმწოდებელთან.

- კიბერთაღლითები ცდილობენ შექმნან ფიქტიური ვებგვერდები, რომლებიც ავთენტურად გამოიყურება. ინფორმაციის შეყვანამდე რამდენჯერმე გადაამოწმეთ ვებგვერდის სანდოობა,[5] განსაკუთრებით იმ შემთხვევაში თუ არ გაქვთ ამ მიმწოდებელთან შესყიდვის გამოცდილება და მისი რეალურობის შესახებ არ გსმენიათ;

> ***როგორ გამოვიყენო ინტერნეტი უსაფრთხოდ?***
>
> ქვემოთმოცემული ქსელის სახეობები დალაგებულია მოწყვლადობის დონის კლების მიხედვით:
>
> - ინტერნეტ-კავშირი (მათ შორს: Wi-Fi, მობილური ინტერნეტი) დაშიფრული VPN *-ის გამოყენებით;
> - მობილური ინტერნეტი;
> - კერძო (სახლის) Wi-Fi;
> - საჯარო (ღია) Wi-Fi.
>
> საჯარო ადგილებში ღია Wi-Fi-ით სარგებლობისას ძალიან მაღალია თქვენს სისტემაში უნებართვოდ შეღწევის რისკი. საჯარო Wi-Fi შესაძლებელია გაზიარებული იყოს ნებისმიერი მავნე აქტორის მიერ, რომელსაც ის გამოიყენებს, მაგალითად, პაროლისა და მომხმარებლის, ან ქსელით გადაცემული სხვა ნებისმიერი ინფორმაციის უნებართვოდ მოსაპოვებლად. აღნიშნულის გათვალისწინებით რეკომენდებულია, მაქსიმალურად მოერიდოთ საჯარო Wi-Fi-ის გამოყენებას.
>
> * ***დაშიფრული ვირტუალური კერძო ქსელი*** **(VPN)** საშუალებას აძლევს მომხმარებლებს გაგზავნონ და მიიღონ პერსონალური მონაცემები საჯარო ქსელში დაშიფრული სახით, რაც უზრუნველყოფს უსაფრთხო კომუნიკაციას და იცავს პერსონალურ მონაცემებს არასათანადო წვდომისგან.

[5] იხილეთ - როგორ შევამოწმო არის თუ არა ვებგვერდი უსაფრთხო?

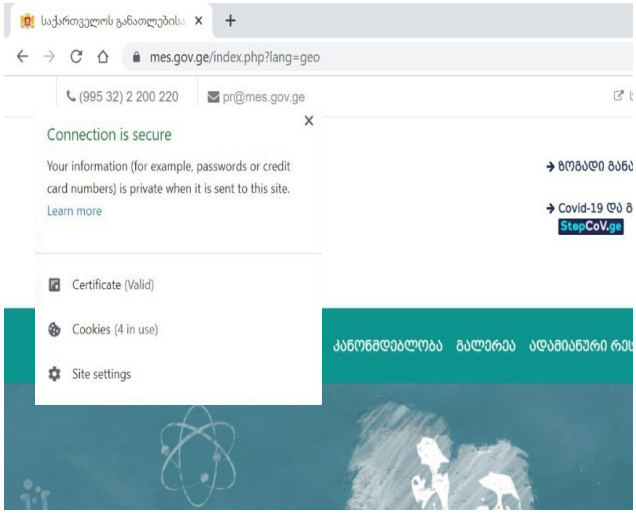
- არ დაუკავშირდეთ დაუცველ საჯარო Wi-Fi-ს[6], განსაკუთრებით შესყიდვების ან საბანკო გადარიცხვების განხორციელებისას.

- ნივთები შეიძინეთ ისეთი ვებგვერდებიდან, რომლებთანაც თქვენი პერსონალური მონაცემების მიმოცვლა ხდება დაშიფრულად. ვებგვერდების უმრავლესობა ინტერნეტის გამოყენებით მონაცემების დაშიფრულად გადაცემისათვის იყენებს მონაცემთა შიფრაციის პროტოკოლს SSL (Secure Sockets Layer[7]). ვებგვერდის უსაფრთხოების შეფასებისას გაითვალისწინეთ, ბმული უნდა იწყებოდეს "https:" და არა "http:" და თან ერთვოდეს ბოქლომის სიმბოლო, რაც მიუთითებს ინფორმაციის დაცულობაზე. ვებგვერდზე, რომელიც არ აკმაყოფილებს უსაფრთხოების მოცემულ მოთხოვნებს, არ გააზიაროთ პერსონალური ან ფინანსური ინფორმაცია ან არ შექმნათ მომხმარებელი.

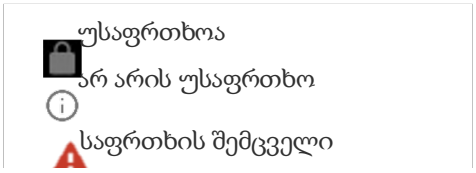
როგორ შევამოწმო არის თუ არა ვებგვერდი უსაფრთხო?

საჩვენებელ ფოტოზე მოცემულია ვებგვერდის უსაფრთხოების შემოწმება Google chrome-ის ბრაუზერის მაგალითზე.

- გახსენით ვებგვერდი ბრაუზერში და დააკვირდით ბმულის მარცხნივ მოცემულ აღნიშვნას;
- დაკლიკეთ აღნიშვნაზე. შედეგად, გამოგიჩნდებათ ინფორმაცია ვებგვერდის უსაფრთხოების სტატუსის შესახებ.



Chrome გვერდის უსაფრთხოების შესაფასებლად იყენებს შემდეგი აღნიშვნებს:



- ვებგვერდზე შეავსეთ მხოლოდ ნივთის შესაძენად საჭირო მონაცემები, რომლებიც აღნიშნულია სავალდებულოდ შესავსებ ველებად და ხშირ შემთხვევაში მოცემულია ვარსკვლავის (*) ნიშნით. სავალდებულო ველებს ძირითადად წარმოადგენს მაიდენტიფიცირებელი ინფორმაცია (მაგ: სახელი, გვარი, პირადი ნომერი), მისამართი (მიტანის სერვისის შემთხვევაში) და ბარათის მონაცემები.

[6] კერძო Wi-Fi არის პირადი მოხმარების პაროლით დაცული ქსელი, ხოლო საჯარო Wi Fi არის საჯარო სივრცეებში გაზიარებული კავშირი.

[7] მონაცემთა შიფრაციის პროტოკოლი (SSL) უზრუნველყოფს უსაფრთხო კავშირს ვებ გვერდის მომხმარებელსა და ვებ-სერვერს შორის. SSL-ის გამოყენებით მონაცემთა გაცვლისას დაცულია კონფიდენციალურობა და უსაფრთხოება.

- ვებგვერდმა შეიძლება მოითხოვოს თქვენი ბარათის მონაცემების შენახვა. არ მონიშნოთ შენახვის შესაბამისი ღილაკი, თუ არ გეგმავთ ონლაინ მაღაზიიდან რეგულარული შესყიდვების განხორციელებას.

8.3. ყურადღებით შეამოწმეთ საეჭვო ელ-ფოსტა, სატელეფონო ზარები და მოკლე ტექსტური შეტყობინებები (SMS)

ონლაინ სივრცეში ვაჭრობისას არაერთ შეტყობინებას მიიღებთ სხვადასხვა ონლაინ მაღაზიიდან. მიღებულ შეტყობინებებს შორის შეიძლება იყოს თქვენი პირადი მონაცემებისა და ფულის მოსაპარად თაღლითურად შექმნილი შეთავაზებები საეჭვო ბმულითა და დანართებით, რომლის გარჩევა რეალური შეთავაზებისგან უფრო და უფრო რთული ხდება.

- არ გახსნათ ვებგვერდის ბმული ან არ გადმოიწეროთ მეილზე მიბმული დანართი თუ არ ხართ დარწმუნებული წყაროს/გამომგზავნის სანდოობაში. ხშირად ელ-ფოსტით მიიღებთ სპეციალურ შეთავაზებებს კომპანიებისგან. კიბერდამნაშავეები ძირითადად ამ მეთოდს იყენებენ და აგზავნიან მეილებს, რომლებიც შეიცავს მავნე დაინფიცირებულ ბმულებს ან გთხოვთ თქვენი პერსონალური მონაცემების ან ფინანსური ინფორმაციის გაზიარებას.

- არ გააზიაროთ თქვენი პაროლი, პერსონალური ან ფინანსური ინფორმაცია ელ-ფოსტის საეჭვო გზავნილის (Spam) საპასუხოდ. რეალურ შემთხვევებში, კომპანიები მომხმარებლისგან არ ითხოვენ მსგავს მონაცემებს ელ-ფოსტის გამოყენებით.

8.4. ისარგებლეთ გადახდის უსაფრთხო მეთოდით

შესყიდვაზე გადაწყვეტილების მიღებისას, პერსონალური ან ფინანსური მონაცემების გაზიარებამდე შეამოწმეთ ვებგვერდის კონფიდენციალობის პოლიტიკა. დარწმუნდით, რომ იცნობთ სპეციფიკას, როგორ ამუშავებს, იყენებს და ინახავს ორგანიზაცია თქვენს მონაცემებს.

- მიზანშეწონილია, გამოიყენოთ გადახდის უსაფრთხო მეთოდები, როგორიც არის ონლაინ გადახდის პლატფორმები (PayPal, Google Pay ან Apple Pay) და ონლაინ ვაჭრობისთვის შექმნილი საბანკო ბარათი, რომელზეც მხოლოდ ვაჭრობისთვის საჭირო თანხა იქნება დარიცხული. ასევე, არ გამოიყენოთ თანხის გადარიცხვის ან ანგარიშსწორების სხვა მეთოდი (მაგ: Bitcoin), რომ არ გაგირთულდეთ თანხის უკან დაბრუნება თაღლითობის შემთხვევაში.

- გადახდაზე გადაწყვეტილების მიღებისას შეამოწმეთ გადახდის გვერდი რამდენად აკმაყოფილებს ვებგვერდის უსაფრთხოების მოთხოვნებს.[8]

- ყურადღებით იყავით ელ-ფოსტით მიღებულ მოთხოვნაზე - გააზიაროთ პირადი მონაცემები. თაღლითებმა შეიძლება გამოგიგზავნონ შეტყობინება მოთხოვნით - დაადასტუროთ გადახდა ან მომხმარებლის ინფორმაცია.

[8] იხილეთ - როგორ შევამოწმო არის თუ არა ვებგვერდი უსაფრთხო?

- არ გაუზიაროთ საბანკო ინფორმაცია (ინტერნეტ ბანკის მომხმარებელი ან პაროლი, ბარათის ნომერი, CVC კოდი, მოქმედების ვადა) სხვა პირს; ხშირია შემთხვევები, როდესაც კიბერთაღლითები ბანკების და სხვა კომპანიების სახელით ითხოვენ პირად ან საბანკო მონაცემებს, თუმცა, გაითვალისწინეთ, მსგავსი ინფორმაციის მოთხოვნის საჭიროება არ არსებობს.

- შესაძლო თაღლითობის გამოსავლენად პერიოდულად შეამოწმეთ საბანკო ამონაწერი, განსაკუთრებით, დღესასწაულების დროს გაზრდილი შესყიდვებისას. საეჭვო შემთხვევების გამოვლენისას დაუყონებლივ შეატყობინეთ მომსახურე ბანკს და შესაძლებლობის შემთხვევაში დაუყოვნებლივ დაბლოკეთ გამოყენებული ბარათი.

გახსოვდეთ! რომ საკუთარი მონაცემების დაცვაში მნიშვნელოვანი ფუნქციის შესრულება შეგიძლიათ. ციფრული ტექნოლოგიების განვითარების ეპოქაში პერსონალური მონაცემების დამუშავებაში თქვენი მონაწილეობა და კონტროლი განსაკუთრებით საჭირო და აუცილებელია. ონლაინ ვაჭრობისას პერსონალური მონაცემების არაკანონიერმა დამუშავებამ შესაძლოა შეუქცევადი ფინანსური ზიანი მოგაყენოთ. ამ რისკების შემცირება კი თქვენს ხელშია.