მუხლი 29 მონაცემთა დაცვის სამუშაო ჯგუფი
Article 29 Data Protection Working Party

01037/12/EN
WP 196

მოსაზრება 05/2012 ღრუბლოვან სისტემაზე

(თარგმანი)

Opinion 05/2012 on Cloud Computing

მიღებულია 2012 წლის პირველ ივლისს

თარგმანის ავტორი: კახაბერ გოშაძე
სამეცნიერო რედაქტორი: მარიამ ბობოხიძე

თბილისი, 2017
გამომცემლობა „ურისტების სამყარო“

გამომცემლობა „იურისტების სამყარო"

თბილისი, მ. კოსტავას #75; ტელ:. 238 35 99; 557 51 51 34
Website: www.law.ge
E-mail: Lawyers.world@yahoo.com;
https://www.facebook.com/PublishingHouselawyersworld

ISBN 978-9941-9537-5-0

სამუშაო ჯგუფი დაფუძნებულია 95/46/EC დირექტივის 29-ე მუხლის საფუძველზე. იგი წარმოადგენს ევროპულ დამოუკიდებელ საკონსულტაციო ორგანოს მონაცემთა დაცვისა და პრივატულობის საკითხებთან დაკავშირებით. მისი მოვალეობები გაწერილია 95/46/EC დირექტივის 30-ე და 2002/58/EC დირექტივის მე-15 მუხლით.

სამდივნო წარმოდგენილია ევროპული კომისიის -C- დირექტორატის (ძირითადი უფლებები და კავშირის მოქალაქეობა) მიერ, მართლმსაჯულების გენრალური დირექტორატი, B-1049 ბრიუსელი, ბელგია, ოფისი MO-59 02/013.

ვებ-გვერდი: http://ec.europa.eu/justice/data-protection/index_en.htm

ევროპული კომისია (European Commission) და მუხლი 29 მონაცემთა დაცვის სამუშაო ჯგუფი (WP29) არ არის პასუხისმგებელი დოკუმენტის სხვა ენაზე თარგმნის ხარისხზე, ასევე, მის შინაარსზე. აღნიშნული თარგმანი ხელმისაწვდომია ნებისმიერი დაინტერესებული პირისთვის და მისი გამოყენება კომერციული მიზნებისთვის აკრძალულია.

მთარგმნელისგან

პერსონალური მონაცემები ექვემდებარება სხვადასხვა მეთოდითა და საშუალებებით დამუშავებას. ამ პროცესში, ტექნოლოგიური საშუალებების განვითარებასთან ერთად, იმატებს მონაცემთა სუბიექტების - ინდივიდების უფლებათა დარღვევის რისკი.

ტექნოლოგიური პროგრესი ქმნის პერსონალურ მონაცემთა მართვის მოქნილ და მოსახერხებელ მეთოდთა ერთობლიობას. სწორედ ასეთ მოქნილ პლატფორმას წარმოადგენს ღრუბლოვანი სისტემა, რომლითაც შესაძლებელია სხვადასხვა ინფორმაციის, მათ შორის, პერსონალური მონაცემების ვირტუალურ მეხსიერებაში (ინტერნეტის მეშვეობით) დამუშავება და შენახვა. ამ მეთოდის ეფექტურობის პარალელურად, აუცილებელია ვუზრუნველყოთ პერსონალურ მონაცემთა შესაბამისი დაცვა და მხოლოდ სათანადო საფუძვლებით დამუშავება, მონაცემთა ტექნიკური უსაფრთხოების მოთხოვნის მკაცრი დაცვით.

პერსონალურ მონაცემთა დაცვის ქართული მოდელი ევროპულ სისტემაზეა აგებული. ამას მოწმობს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის ტექსტი, ასევე, საქართველოსა და ევროპულ კავშირს შორის გაფორმებული ასოცირების შეთანხმების მე-14 მუხლი, რის

მიხედვითაც, მონაცემთა დაცვის ქართული მოდელი უნდა შეესაბამებოდეს ევროპულ კავშირში მოქმედი 95/46/EC დირექტივით (მონაცემთა დაცვის დირექტივა) დადგენილ სტანდარტებს.

საქართველოში პერსონალურ მონაცემთა დაცვასთან დაკავშირებული ურთიერთობები სამართლებრივად შედარებით გვიან მოწესრიგდა, ვიდრე ეს მოხდა ევროპაში, თუმცა ის სირთულეები, რაც თან ახლავს ტექნოლოგიური საშუალებებით, კერძოდ, ღრუბლოვანი სისტემით მონაცემთა დამუშავებას, რჩება გამოწვევად ქართველი დამმუშავებლისთვის. შესაბამისად, წინამდებარე თარგმანი დაეხმარება ღრუბლოვან სისტემაში პერსონალურ მონაცემთა დამუშავებით დაინტერესებულ ნებისმიერ პირს სამართლებრივად სწორი გადაწყვეტილების მოძიებასა და მონაცემთა სუბიექტის უფლებათა დაცვაში.

ასევე, მსურს მადლობა გადავუხადო მარიამ ბობოხიძეს თარგმანის სამეცნიერო რედაქტირებისთვის და გამომცემლობა "იურისტების სამყაროს" სამუშაო ჯგუფს თარგმანის გამოცემისთვის.

შენიშვნა:

წინამდებარე მოსაზრება, ინგლისურ ენაზე, გამოცემულია 2012 წლის პირველ ივლისს. ამ დროს, ევროპულ კავშირსა და აშშ-ს შორის ჯერ კიდევ

მოქმედებდა Safe Harbor შეთანხმება. მას შემდეგ, რაც მართლმსაჯულების ევროპული კავშირის სასამართლოს დიდმა პალატამ 2015 წლის 6 ოქტომბერს აღნიშნული შეთანხმება ძალადაკარგულად ცნო (საქმე Maximilian Schrems v. Data Protection Commissioner, C-362/14), ევროპულ კავშირსა და აშშ-ს შორის 2016 წლის 12 ივლისს გაფორმდა ახალი შეთანხება - EU-US Privacy Shield.

მიუხედავად ამ ცვლილებისა, დოკუმენტის ნაწილი, სადაც საუბარია Safe Harbor შეთანხმებაზე, გავლენას არ ახდენს დოკუმენტში მოცემულ მთავარ მიდგომებსა და საკვანძო საკითხებზე.

სარჩევი

რეზიუმე

წინამდებარე მოსაზრებაში, მუხლი 29 სამუშაო ჯგუფი განიხილავს ყველა შესაბამის საკითხს, რომელიც ეხება ღრუბლოვანი სისტემის (Cloud Computing) მომსახურების მომწოდებლებს ევროპის ეკონომიკურ ზონაში (EEA) და მათ მომხმარებლებს, ასევე, განსაზღვრავს ევროპული კავშირის მონაცემთა დაცვისა (95/46/EC) და, საჭიროების შემთხვევაში, 2002/58/EC ელ-პრივატულობის დირექტივიდან (გადასინჯული 2009/136/EC საფუძველზე) გამომდინარე პრინციპებს.

მიუხედავად ღრუბლოვანი სისტემის აღიარებული უპირატესობებისა, როგორც ეკონომიკური, ასევე სოციალური თვალსაზრისით, წინამდებარე მოსაზრება ასახავს, თუ როგორ შეუძლია ღრუბლოვანი სისტემის მომსახურებების ფართო გავრცელებამ ბიძგი მისცეს არაერთ რისკს მონაცემთა დაცვის მხრივ, რაც ძირითადად, გამოიხატება პერსონალურ მონაცემთა მიმართ კონტროლის დაკარგვაში, ასევე, არასაკმარის ინფორმაციაში იმის შესახებ, თუ როგორ, სად და ვის მიერ ხდება მონაცემთა დამუშავება/ქვე-დამუშავება. აღნიშნული რისკები საჯარო უწყებებისა და კერძო დაწესებულებების მიერ სიფრთხილით უნდა შეფასდეს თუ ისინი განიხილავენ ღრუბლოვანი სისტემის მომწოდებლის მომსახურებების გამოყენებას. ამ მოსაზრებაში განხილულია საკითხები,

რომელიც ეხება სხვა პირებისთვის რესურსების განაწილებას, აუთსორსის სისტემის გამჭვირვალობის ნაკლებობას, სადაც მოცემულია მრავალი უფლებამოსილი პირი და ქვე-კონტრაქტორი, ასევე, მონაცემთა საერთო გლობალური რეგულაციის არარსებობასა და ევროპის ეკონომიკური ზონის ფარგლებს გარეთ დაფუძნებული ღრუბლოვანი სისტემის მომწოდებლებისთვის პერსონალურ მონაცემთა გადაცემასთან დაკავშირებულ უზუსტობებს. მსგავსად ამისა, მოსაზრებაში, მნიშვნელოვანი ყურადღების საგნად, ხაზგასმულია გამჭვირვალობის ნაკლებობა იმ მხრივ, თუ რა ინფორმაციის მიწოდების ვალდებულება აქვს მონაცემთა დამმუშავებელს მონაცემთა სუბიექტისთვის, მის შესახებ მონაცემთა დამუშავებისას. მონაცემთა სუბიექტები უნდა[1] იყვნენ ინფორმირებულები, თუ ვინ და რა მიზნისთვის ამუშავებს მათ მონაცემს და ჰქონდეთ შესაძლებლობა, მოახდინონ ამ მხრივ მინიჭებული უფლებების რეალიზაცია.

ამ მოსაზრების მთავარი დასკვნა არის ის, რომ იმ კომპანიებმა და დაწესებულებებმა, რომლებსაც სურთ ღრუბლოვანი სისტემის გამოყენება, უპირველეს ყოვლისა, უნდა განახორციელონ რისკების

1 ინგლისურენოვან ვერსიაში სიტყვები "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", და "OPTIONAL" უნდა განიმარტოს, როგორც აღწერილია დოკუმენტში 2119. დოკუმენტი ხელმისაწვდომია ბმულზე http://www.ietf.org/rfc/rfc2119.txt.

სრულყოფილი და ღრმა ანალიზი. ევროპის ეკონომიკურ ზონაში ღრუბლოვანი სისტემის მომსახურების ყველა მწარმოებელმა უნდა მოახდინოს ღრუბლოვანი სისტემის მომხმარებელთა ინფორმირება ყველა იმ დეტალურ საკითხთან დაკავშირებით, რომელიც აუცილებელია ამ სისტემის დანერგვის დადებითი და უარყოფითი მხარეების სწორად შეფასებისთვის. უსაფრთხოება, გამჭვირვალობა და სამართლებრივი სიზუსტე უნდა იყოს მთავარი ფაქტორი მომხმარებელთა არჩევანისთვის, რომელიც დგას ღრუბლოვანი სისტემის მომსახურების შესახებ შეთავაზების მიღმა.

ამ მოსაზრებაში მოცემული რეკომენდაციების გათვალისწინებით, ხაზგასმულია ღრუბლოვანი სისტემის მომხმარებლის, როგორც მონაცემთა დამმუშავებლის ვალდებულებები და, შესაბამისად, რეკომენდირებულია, რომ მომხმარებელმა არჩევანი შეაჩეროს ღრუბლოვანი სისტემის იმ მომწოდებელზე, რომელიც უზრუნველყოფს შესაბამისობას ევროპული კავშირის მონაცემთა დაცვის კანონმდებლობასთან. ამ მოსაზრებაში, ასევე, განხილულია უსაფრთხოების შესაბამისი სახელშეკრულებო პირობები, რომლის მიხედვით, ღრუბლოვანი სისტემის მომხმარებელსა და მის მომწოდებელს შორის გაფორმებული ნებისმიერი ხელშეკრულება უნდა ადგენდეს ტექნიკური და ორგანიზაციული უსაფრთხოების ადეკვატურ

გარანტიებს. აგრეთვე მნიშვნელოვანია, რომ ღრუბლოვანი სისტემის მომხმარებლებმა გადაამოწმონ, თუ რამდენად შეუძლია ღრუბლოვანი სისტემის მომწოდებელს მონაცემთა ტრანსსასაზღვრო, საერთაშორისო გადაცემის კანონიერების უზრუნველყოფა.

ნებისმიერი ევოლუციური პროცესის მსგავსად, ღრუბლოვანი სისტემის განვითარება, როგორც გლობალური ტექნოლოგიური პარადიგმა, წარმოადგენს გამოწვევას. ეს მოსაზრება, წინამდებარე სახით, შესაძლებელია ჩაითვალოს მნიშვნელოვან ნაბიჯად იმ ვალდებულებათა განსაზღვრისთვის, რომელიც მომდევნო წლებში უნდა გაითვალისწინოს მონაცემთა დაცვის თანამეგობრობამ.

1. შესავალი

ზოგისთვის, ღრუბლოვანი სისტემა არის ტექნოლოგიური რევოლუციის ერთ-ერთი უდიდესი მიღწევა, რომელსაც მცირე ხნის წინ ჰქონდა ადგილი. სხვებისთვის, ის უბრალოდ ტექნოლოგიური საშუალებების ბუნებრივი განვითარების შედეგია, რომელიც მიზნად ისახავს მიაღწიოს კომპიუტერული სისტემების მაქსიმალურ სასურველ პროდუქტიულობას. ნებისმიერ შემთხვევაში, მონაწილეთა დიდმა ნაწილმა საკუთარი ტექნოლოგიური სტრატეგიების განვითარებაში წინა პლანზე წამოწია ღრუბლოვანი სისტემა.

ღრუბლოვანი სისტემა შედგება ტექნოლოგიური საშუალებების ნაკრებისა და მომსახურების ფორმებისგან, რომელიც აქცენტირებულია ინფორმაციული ტექნოლოგიების (IT) აპლიკაციების, დამუშავების შესაძლებლობების, შენახვისა და მეხსიერების ადგილის ინტერნეტის მეშვეობით მიწოდებაზე. ღრუბლოვანი სისტემა შესაძლებელია იყოს მნიშვნელოვანი ეკონომიკური სარგებლის მომტანი, რამდენადაც მოთხოვნაზე დაფუძნებული რესურსების ფორმირება, ინტერნეტის მეშვეობით მისი გავრცობა და მისაწვდომობა, საკმაოდ მარტივად განხორციელებადია. ეკონომიკურ სარგებელთან ერთად, ღრუბლოვანი სისტემა შესაძლებელია, ასევე, აღმოჩნდეს პროდუქტიული უსაფრთხოების მხრივ; კომპა-

ნიებს, განსაკუთრებით მცირესა და საშუალოს, შეუძლიათ მინიმალური დანახარჯებით მიიღონ უმაღლესი დონის ტექნოლოგიები, რომელიც სხვა მხრივ, მათი ბიუჯეტის გათვალისწინებით, მიუღწეველი იქნება.

ღრუბლოვანი სისტემის მომწოდებლებისგან შემოთავაზებული მომსახურებების ფართო დიაპაზონი არსებობს, დაწყებული დამუშავების ვირტუალური სისტემებით (რომელიც ანაცვლებს ან/და ფუნქციონირებს ჩვეულებრივ სერვერებთან ერთად, დამმუშავებლის პირდაპირი კონტროლის ქვეშ), ასევე სერვისებით, რომელიც ითვალისწინებს აპლიკაციების დამუშავებასა და ფუნქციურ ჰოსტინგს, დამთავრებული ვებზე დაფუძნებული პრორგამული საშუალებებით, რომლებსაც შეუძლიათ ჩაანაცვლონ საბოლოო მომხმარებლის პერსონალურ კომპიუტერებზე ინსტალირებული ჩვეულებრივი აპლიკაციები. იგი მოიცავს ტექსტის დამუშავებისათვის არსებულ პროგრამულ უზრუნველყოფებს, დამგეგმავებსა და კალენდრებს, ფაილურ სისტემებს დოკუმენტების ონლაინ შენახვისთვის და აუთსორსირებული ელექტრონული ფოსტის საშუალებებს. აღნიშნული განსხვავებული სერვისების განსამარტად, ზოგიერთი, ყველაზე ხშირად გამოყენებული ცნება, მოცემულია ამ მოსაზრების დანართით.

მოსაზრებაში მუხლი 29 სამუშაო ჯგუფი (შემდგომში – WP29) განიხილავს ევროპულ ეკონომიკურ ზონაში (შემდგომში – EEA) მოქმედ კანონმდებლობას, ვალდებულებებს დამმუშავებლებისთვის და ღრუბლოვანი სისტემის მომწოდებლების ვალდებულებებს კლიენტების მიმართ EEA-ში. ეს მოსაზრება ფოკუსირებულია ვითარებაზე, როდესაც ურთიერთობა ყალიბდება დამმუშავებელსა და უფლებამოსილ პირს შორის, სადაც მომხმარებელი მიჩნეულია დამმუშავებლად, ხოლო ღრუბლოვანი სისტემის მომწოდებელი – უფლებამოსილ პირად. იმ შემთხვევებში, როდესაც ღრუბლოვანი სისტემის მომწოდებელი მოქმედებს როგორც დამმუშავებელი, მან უნდა შეასრულოს დამატებითი ვალდებულებები. შედეგად, მონაცემთა დამმუშავებლისთვის ღრუბლოვანი სისტემის გამოყენების წინაპირობას წარმოადგენს რისკების ადეკვატური შეფასება, რომელიც მოიცავს იმ სერვერების ადგილმდებარეობის დადგენას, სადაც ხდება მონაცემთა დამუშავება, ასევე, მონაცემთა დაცვის პერსპექტივიდან გამომდინარე რისკებისა და სარგებლის გააზრება, მომდევნო პარაგრაფებში მოცემული კრიტერიუმების შესაბამისად.

აღნიშნული მოსაზრება განსაზღვრავს მოქმედ პრინციპებს როგორც მონაცემთა დამმუშავებლების, ისე უფლებამოსილი პირებისთვის, რომელიც

მომდინარეობს მონაცემთა დაცვის ძირითადი დირექტივიდან (95/46/EC), კერძოდ, მიზნის კონკრეტულობა და ლიმიტირება, მონაცემთა წაშლა, ტექნიკური და ორგანიზაციული ზომები. მოსაზრება წარმოადგენს სახელმძღვანელოს უსაფრთხოების მოთხოვნებისთვის, როგორც სტრუქტურულ ასევე პროცედურულ საკითხებზე. განსაკუთრებით ხაზგასმულია სახელშეკრულებო შეთანხმებები, რითაც უნდა დარეგულირდეს ურთიერთობა დამმუშავებელსა და უფლებამოსილ პირს შორის. მონაცემთა დაცვის კლასიკურ მიზნებს წარმოადგენს ხელმისაწვდომობა, მთლიანობა და კონფიდენციალურობა. მიუხედავად ამისა, მონაცემთა დაცვა არ არის დაყვანილი მხოლოდ მონაცემთა უსაფრთხოებამდე და, შესაბამისად, ეს მიზნები თანმდევია მონაცემთა დაცვის ისეთი სპეციფიკური მიზნებისა, როგორიცაა გამჭვირვალობა, განცალკევება, ჩარევაუნარიანობა და პორტატულობა, რათა უზრუნველყოფილი იყოს ადამიანის უფლებათა ევროპული ქარტიით განმტკიცებული ინდივიდის უფლება მონაცემთა დაცვაზე.

EEA-ს ფარგლებს გარეთ მონაცემთა გადაცემასთან დაკავშირებით გაანალიზებულია ისეთი ინსტრუმენტები, როგორიცაა ევროპული კომისიის მიერ მიღებული ხელშეკრულების სტანდარტული პირობები, ადეკვატურობის დადგენა და სავალდებულო საკორპორაციო წესები (BCR) სავარაუ-

დო, სამომავლო უფლებამოსილი პირისთვის. ასევე განხილულია რისკები, რომელიც წარმოიშობა საერთაშორისო სამართალდამცავი ორგანოების მოთხოვნათა გამო.

დასკვნის სახით, მოსაზრება აყალიბებს რეკომენდაციებს ღრუბლოვანი სისტემის მომხმარებლებისთვის, როგორც დამმუშავებლებისთვის, ხოლო ღრუბლოვანი სისტემის მომწოდებლებისთვის, როგორც უფლებამოსილი პირებისთვის, ასევე, ევროპული კომისიისთვის, მონაცემთა დაცვის ევროპული რეგულაციის სამომავლო ცვლილებების გათვალისწინებით.

სატელეკომუნიკაციო სფეროში მონაცემთა დაცვის ბერლინის საერთაშორისო სამუშაო ჯგუფმა 2012 წლის აპრილში მიიღო Sopot მემორანდუმი.[2] აღნიშნული მემორანდუმი განიხილავს პრივატულობისა და მონაცემთა დაცვის საკითხებს ღრუბლოვან სისტემაში და ხაზს უსვამს იმას, რომ მონაცემთა დამუშავების ჩვეულებრივ პროცესთან შედარებით, ღრუბლოვანმა სისტემამ არ უნდა გამოიწვიოს მონაცემთა დაცვის სტანდარტების დაქვეითება.

---

2 http://datenschutz-berlin.de/attachments/873/Sopot_Memorandum_Cloud_Computing.pdf.

2. მონაცემთა დაცვის რისკები ღრუბლოვან სისტემაში

წინამდებარე მოსაზრება აქცენტირებულია ღრუბლოვანი სისტემის მომსახურებების მეშვეობით მონაცემთა დამუშავებაზე, შესაბამისად, ყურადღება გამახვილდება მხოლოდ კონკრეტულ კონტექსტუალურ რისკებზე.[3] ამ რისკების უმრავლესობა ერთიანდება ორ ძირითად კატეგორიაში, კერძოდ, მონაცემთა კონტროლის ნაკლებობა და არასაკმარისი ინფორმაცია მონაცემთა დამუშავების პროცესის შესახებ (გამჭვირვალობის არარსებობა). ამ მოსაზრებაში მიმოხილული, ღრუბლოვან სისტემასთან დაკავშირებული, კონკრეტული რისკები მოიცავს შემდეგ საკითხებს:

კონტროლის ნაკლებობა

პერსონალური მონაცემების იმ სისტემებისთვის გადაცემით, რომელიც მართულია ღრუბლოვანი სისტემის მომწოდებლის მიერ, ღრუბლოვანი სისტემის მომხმარებლებს შესაძლოა აღარ გააჩნდეთ აღნიშნული მონაცემების ექსკლუზიური კონტროლის შესაძლებლობა და ვერ დანერგონ ტექნიკური და ორგანიზაციული ზომები, რომელიც

3 ღრუბლოვან სისტემაში მონაცემთა დამუშავების რისკებთან ერთად, რომელიც არის ნახსენები ამ მოსაზრებაში, მხედველობაში ასევე უნდა იქნას მიღებული ყველა ის რისკი, რომელიც ეხება პერსონალურ მონაცემთა დამუშავებას აუთსორსის მეშვეობით.

აუცილებელია მონაცემთა ხელმისაწვდომობის, მთლიანობის, კონფიდენციალურობის, გამჭვირვალობის, განცალკევების,[4] ჩარევაუნარიანობისა და პორტატულობისთვის. კონტროლის აღნიშნულმა ნაკლოვანებებმა შესაძლოა შემდეგ ფორმებში იჩინოს თავი:

- ხელმისაწვდომობის ნაკლებობა ფუნქციური თავსებადობის ნაკლებობის გამო (ერთ მომწოდებელზე მიბმა): თუ ღრუბლოვანი სისტემის მომწოდებელი იყენებს მესაკუთრეობრივი ფუნქციის მქონე ტექნოლოგიას, ღრუბლოვანი სისტემის მომხმარებლისთვის შესაძლებელია რთული აღმოჩნდეს მონაცემთა და დოკუმენტთა გადაადგილება სხვადასხვა ღრუბლოვან სისტემას შორის (მონაცემთა პორტატულობა) ან მონაცემთა გაცვლა იმ პირებთან, რომლებიც იყენებენ სხვადასხვა მომწოდებლის მიერ ადმინისტრირებულ ღრუბლოვან სერვისებს (შეთავსებადობა).
- რესურსების გაზიარებით გამოწვეული მთლიანობის ნაკლებობა: ღრუბლოვანი სისტემა შედგება გაზიარებული სისტემებისა და ინფრასტრუქტურისგან. ღრუბლოვანი სისტემის მომწოდებლები ამუშავებენ პერსონალურ მონაცემებს, რომელიც მომდინარეობს მრავალი წყაროდან, მონაცემთა სუბიექტებისა და ორგანიზაციების გათვალისწინებით, რა

4 გერმანიაში „დაუკავშირებლობის“ ფართო კონცეფცია იქნა წარმოდგენილი. იხ. fn. 24.

დროსაც არსებობს ინტერესთა კონფლიქტის ან/და სხვა მიზნების წარმოშობის შესაძლებლობა.

- კონფიდენციალურობის ნაკლებობა სამართალდამცავი ორგანოების მხრიდან არსებული მონაცემთა დამუშავების მოთხოვნების გათვალისწინებით, რაც წარედგინება უშუალოდ ღრუბლოვანი სისტემის მომწოდებელს: პერსონალური მონაცემები, რომელიც მუშავდება ღრუბლოვან სისტემაში შესაძლებელია გახდეს ევროპული კავშირის წევრი ქვეყნებისა და მესამე ქვეყნების სამართალდამცავი ორგანოების მხრიდან კანონის აღსრულების მიზნით არსებული მოთხოვნების ობიექტი. არსებობს პერსონალური მონაცემების (უცხო ქვეყნის) სამართალდამცავი ორგანოებისთვის გამჟღავნების რისკი, ევროპული კავშირის ფარგლებში არსებული შესაბამისი სამართლებრივი საფუძვლის გარეშე, რაც, თავის მხრივ, არღვევს ევროპული კავშირის მონაცემთა დაცვის კანონმდებლობას.
- ჩარევაუნარიანობის ნაკლებობა აუთსორსის სისტემის კომპლექსურობისა და დინამიურობის გამო: ერთი კონკრეტული მომწოდებლის მიერ შემოთავაზებული ღრუბლოვანი სისტემის მომსახურება შესაძლოა დაფუძნებული იყოს კომბინირებულ მომსახურებებზე, რომელიც შემოთავაზებულია სხვადასხ-

ვა მომწოდებლების მიერ. მომხმარებელთან ხელშეკრულების მოქმედების განმავლობაში, აღნიშნულს, შესაძლებელია დინამიურად ემატებოდეს ან აკლდებოდეს გარკვეული მომსახურება.

- ჩარევაუნარიანობის ნაკლებობა (მონაცემთა სუბიექტების უფლებები): ღრუბლოვანი სისტემის მომწოდებელმა შესაძლოა არ დანერგოს აუცილებელი ზომები და საშუალებები, რათა დახმარება გაუწიოს დამმუშავებელს მონაცემთა მართვასთან დაკავშირებით, მაგ. წდვომის, წაშლის ან მონაცემთა შესწორების უზრუნველსაყოფად.
- განცალკევების ნაკლებობა: ღრუბლოვანი სისტემის მომწოდებელი შესაძლოა იყენებდეს ფიზიკურ კონტროლს სხვადასხვა მომხმარებლის მიერ მოწოდებულ მონაცემებზე, რათა ერთმანეთთან დააკავშიროს პერსონალური მონაცემები. თუ ადმინისტრატორებს მინიჭებული აქვთ წვდომის საკმაოდ პრივილეგირებული უფლებები (მაღალი რისკის მატარებლები), მათ შეუძლიათ დააკავშირონ სხვადასხვა მომხმარებლის ინფორმაცია.

დამუშავების შესახებ ინფორმაციის ნაკლებობა (გამჭვირვალობა)

ღრუბლოვანი სისტემის მომსახურებების ფუნქციონირების შესახებ არასაკმარისი ინფორმაცია დამმუშავებლებისთვის და ასევე მონაცემთა სუბიექტებისთვის წარმოშობს რისკს, რამდენადაც მათ შესაძლოა არ ჰქონდეთ ინფორმაცია პოტენციური საშიშროებებისა და რისკების შესახებ, შესაბამისად, ვერ მიიღონ ზომები, რომელსაც საჭიროდ მიიჩნევენ.

ზოგიერთი პოტენციური საფრთხე შესაძლოა წარმოიშვას იქედან, რომ დამმუშავებელმა არ იცოდეს შემდეგის არსებობა:

- აქვს ადგილი ქსელურ დამუშავებას, რომელიც მოიცავს მრავალ უფლებამოსილ პირსა და ქვე-კონტრაქტორს.
- პერსონალურ მონაცემთა დამუშავება ხდება სხვადასხვა გეოგრაფიულ ადგილას **EEA**-ს ფარგლებში. ეს პირდაპირ ახდენს გავლენას მოქმედ სამართალზე, როდესაც წარმოიშობა დავა მომხმარებელსა და მომწოდებელს შორის მონაცემთა დაცვასთან დაკავშირებით.
- პერსონალური მონაცემები გადაიცემა მესამე ქვეყნებისთვის EEA-ს ფარგლებს გარეთ. მესამე ქვეყნები შესაძლოა არ უზრუნველყოფდნენ მონაცემთა დაცვის ადეკვატურ დონეს

და გადაცემა არ იყოს დაცული ადეკვატური ზომებით (მაგ. სტანდარტული სახელშეკრულებო პირობები ან BCR), შესაბამისად, იყოს უკანონო.

დანაწესი, რომლის თანახმად, მონაცემთა სუბიექტები, რომელთა პერსონალური მონაცემების დამუშავება ხდება ღრუბლოვან სისტემაში, უნდა იყვნენ ინფორმირებულები მონაცემთა დამმუშავებლის ვინაობისა და დამუშავების მიზნის შესახებ, წარმოადგენს ვალდებულებას (მსგავსი ვალდებულებაა ყველა დამმუშავებლის მიმართ მონაცემთა დაცვის 95/46/EC დირექტივის თანახმად). ღრუბლოვანი სისტემის გარემოში დამუშავების პოტენციურად კომპლექსური ქსელის გათვალისწინებით, მონაცემთა სუბიექტებს, დამუშავების პროცესის სამართლიანობის უზრუნველსაყოფად (95/46/EC დირექტივის მე-10 მუხლი), დამმუშავებლებმა, საუკეთესო მაგალითის გათვალისწინებით, უნდა მიაწოდონ ინფორმაცია, რომელიც ეხება ღრუბლოვანი სისტემის მომსახურებების წარმოებისას არსებულ (ქვე) დამმუშავებლებს.

3. სამართალებრივი მოწესრიგება

3.1 მონაცემთა დაცვის რეგულაცია

მონაცემთა დაცვას სამართლებრივად აწესრიგებს მონაცემთა დაცვის 95/46/EC დირექტივა. აღნიშნული დირექტივა გამოიყენება ყველა შემთხვევაში, სადაც ხდება პერსონალურ მონაცემთა დამუშავება ღრუბლოვანი სისტემის მომსახურებების გამოყენებით. ელ-პრივატულობის 2002/58/EC დირექტივა (შესწორებული 2009/136/EC თანახმად) გამოიყენება პერსონალურ მონაცემთა დამუშავებისას საჯაროდ ხელმისაწვდომი ელექტრონული კომუნიკაციების მომსახურებების მეშვეობით (ტელეკომ ოპერატორები), შესაბამისად დირექტივა გამოიყენება თუ აღნიშნული სერვისები ფუნქციონირებს ღრუბლოვანი სისტემის გამოყენებით.[5]

5 2002/58/EC ელ-პრივატულობის დირექტივის (ცვლილება იქნა შეტანილი 2009/136/EC დირექტივით) შესახებ: 2002/58/EC დირექტივა პრივატულობის შესახებ სატელეკომუნიკაციო სფეროში ვრცელდება ელექტრონული კომუნიკაციების სერვისების მომწოდებლებზე, რომელიც საჯაროდ არის ხელმისაწვდომი და ავალდებულებს მათ უზრუნველყონ პერსონალურ მონაცემთა და კომუნიკაციების სიდუმლოობა, ასევე განუსაზღვრავს მათ უფლებებსა და ვალდებულებებს ელექტორნული კომუნიკაციების ქსელთან და სერვისებთან დაკავშირებით. იმ შემთხვევაში, როდესაც ღრუბლოვანი სისტემის მომწოდებლები მოქმედებენ როგორც საჯაროდ ხელმისაწვდომი ელექტრონული კომუნიკაციის სერვისების მომწოდებლები, ისინი ექვემდებარებიან ამ დირექტივას.

3.2 მოქმედი სამართალი

მოქმედი სამართლის დადგენის კრიტერიუმები მოცემულია 95/46/EC დირექტივის მე-4 მუხლით, რომელიც ეხება საკითხს, თუ რომელი სამართალი უნდა გამოიყენებოდეს იმ დამმუშავებელზე,[6] რომელსაც გააჩნია ერთზე მეტი დაფუძნების ადგილი EEA-ში და ასევე საკითხს, თუ რომელი სამართალი უნდა გამოიყენებოდეს იმ დამმუშავებლებზე, რომლებიც არიან EEA-ს ფარგლებს გარეთ, თუმცა მონაცემთა დამუშავებისთვის იყენებენ EEA-ს ფარგლებში მდებარე აღჭურვილობას. WP29-მ გააანალიზა აღნიშნული საკითხი თავის მოსაზრებაში 8/2010 მოქმედი სამართლის შესახებ.[7]

პირველ შემთხვევაში, მთავარი ფაქტორი, რაც ბიძგს აძლევს ევროპული კავშირის სამართლის გამოყენებას მონაცემთა დამმუშავებლის მიმართ არის მისი დაფუძნების ადგილი და ქმედებები, რასაც იგი ახორციელებს დირექტივის მე-4(1) მუხლის -a- ქვეპუნქტის თანახმად, რა დროსაც ღრუბლოვანი სისტემის მომსახურების მოდელს არ აქვს მნიშვნელობა. მოქმედია იმ ქვეყნის კანონმდებლობა, სადაც ღრუბლოვანი სისტემის

6 დამმუშავებლის განმარტება მოცემულია დირექტივის მე-2 მუხლის „ჰ“ ქვეპუნქტით და იყო განხილული WP29-ს მიერ თავის მოსაზრებაში 1/2010 დამმუშავებლისა და უფლებამოსილი პირის ცნების შესახებ.

7 http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf.

მომსახურებების შესახებ ხელშეკრულების დამდები დამმუშავებელი არის დაფუძნებული, და არა იმ ქვეყნის კანონმდებლობა, სადაც ღრუბლოვანი სისტემის მომწოდებელი მდებარეობს.

თუ დამმუშავებელი იქნება დაფუძნებული სხვადასხვა წევრ სახელმწიფოში და მონაცემთა დამუშავება მისი საქმიანობის ნაწილი იქნება ამ ქვეყნებში, მოქმედი სამართალი იქნება ყველა იმ წევრი ქვეყნის სამართალი, სადაც ხდება დამუშავება.

მე-4(1) მუხლის -c-[8] ქვეპუნქტი ეხება შემთხვევას, თუ როგორ ვრცელდება მონაცემთა დაცვის კანონმდებლობა იმ დამმუშავებლებზე, რომლებიც არ არიან დაფუძნებულები EEA-ში, მაგრამ იყენებენ წევრი ქვეყნის ტერიტორიაზე მდებარე ავტომატიზებულ ან არაავტომატიზებულ აღჭურვილობას, გარდა იმ შემთხვევისა თუ ეს აღჭურვილობა გამოიყენება ტრანზიტისთვის. ეს ნიშნავს, რომ თუ ღრუბლოვანი სისტემის მომხმარებელი არის დაფუძნებული EEA-ს ფარგლებს გარეთ, მაგრამ იყენებს ღრუბლოვანი სისტემის მომწო-

8 მე-4(1) მუხლის -c- ქვეპუნქტი ადგენს, რომ წევრი ქვეყნის კანონმდებლობა გამოიყენება მაშინ, როდესაც „დამმუშავებელი არ არის დაფუძნებული თანამეგობრობის ტერიტორიაზე და, პერსონალურ მონაცემთა დამუშავების მიზნებისთვის, იყენებს აღჭურვილობას, ავტომატიზებულს ან სხვაგვარს, რომელიც მდებარეობს მოცემული წევრი ქვეყნის ტერიტორიაზე, გარდა იმ შემთხვევისა, როდესაც ეს აღჭურვილობა გამოიყენება მონაცემთა ტრანზიტისთვის თანამეგობრობის ტერიტორიაზე.“

დებელს დაფუძნებულს EEA-ში, მომწოდებელი ახორციელებს მონაცემთა დაცვის კანონმდებლობის ექსპორტს მომხმარებელზე.

3.3 სხვადასხვა მონაწილეთა მოვალეობები და პასუხისმგებლობა

როგორც ზემოთ აღინიშნა, ღრუბლოვანი სისტემა მოიცავს სხვადასხვა მონაწილეებს. მნიშვნელოვანია შეფასდეს და განიმარტოს ყველა ამ მონაწილის როლი, რათა დადგინდეს მათი კონკრეტული ვალდებულებები მონაცემთა დაცვის არსებული კანონმდებლობის გათვალისწინებით.

უნდა აღინიშნოს, რომ WP29-მ თავის მოსაზრებაში 1/2010 დამმუშავებლისა და უფლებამოსილი პირის ცნების შესახებ აღნიშნა, რომ *„პირველი და უმთავრესი პირობა დამმუშავებლის ცნებისთვის არის ის, რომ განისაზღვროს თუ ვინ არის პასუხისმგებელი მონაცემთა დაცვის წესების შესრულებაზე და როგორ ახდენენ უფლებების რეალიზაციას მონაცემთა სუბიექტები. სხვა სიტყვებით: განისაზღვროს პასუხისმგებლობა.“* აღნიშნული ორი ძირითადი კრიტერიუმი, პასუხისმგებლობა დაცვაზე და პასუხისმგებლობის განსაზღვრა, ამ საკითხის ანალიზისას მხარეებმა უნდა გაითვალისწინონ.

3.3.1 ღრუბლოვანი სისტემის მომხმარებელი და ღრუბლოვანი სისტემის მომწოდებელი

ღრუბლოვანი სისტემის მომხმარებელი განსაზღვრავს დამუშავების მთავარ მიზანს და წყვეტს დამუშავების პროცესის აუთსორსს, მის ნაწილობრივ ან სრულ დელეგირებას გარე ორგანიზაციაზე. შესაბამისად, ღრუბლოვანი სისტემის მომხმარებელი მოქმედებს როგორც მონაცემთა დამმუშავებელი. დირექტივა შემდეგი სახით განმარტავს დამმუშავებელს: *„ფიზიკური ან იურიდიული პირი, სახელმწიფო დაწესებულება, სააგენტო ან ნებისმიერი სხვა ორგანო, რომელიც დამოუკიდებლად ან სხვებთან ერთად განსაზღვრავს პერსონალურ მონაცემთა დამუშავების მიზნებსა და საშუალებებს.“* ღრუბლოვანი სისტემის მომხმარებელმა, როგორც დამმუშავებელმა, უნდა აიღოს საკუთარ თავზე პასუხისმგებლობა და დაიცვას მონაცემთა დაცვის წესები, რის თანახმადაც იგი პასუხისმგებელია 95/46/EC დირექტივით მოცემული ყველა ნორმის შესრულებაზე. ღრუბლოვანი სისტემის მომხმარებელმა შესაძლებელია დაავალოს ღრუბლოვანი სისტემის მომწოდებელს, რომ მომხმარებელს დამუშავების მიზნის მისაღწევად ჰქონდეს არჩევანის საშუალება აუცილებელი ტექნიკური და ორგანიზაციული მეთოდების გამოყენებასთან დაკავშირებით.

ღრუბლოვანი სისტემის მომწოდებელი არის პირი,

რომელიც ახორციელებს ღრუბლოვანი სისტემის მომსახურებებს სხვადასხვა ფორმით. როდესაც ღრუბლოვანი სისტემის მომწოდებელი ღრუბლოვანი სისტემის მომხმარებლისთვის იყენებს საშუალებებს და პლატფორმას, ღრუბლოვანი სისტემის მომწოდებელი მიიჩნევა უფლებამოსილ პირად, ესე იგი, 95/46/EC დირექტივის თანახმად არის: *„ფიზიკური ან იურიდიული პირი, საჯარო დაწესებულება, სააგენტო ან ნებისმიერი სხვა ორგანო, რომელიც დამოუკიდებლად ან სხვებთან ერთად, ამუშავებს პერსონალურ მონაცემებს მონაცემთა დამმუშავებლისთვის.“*[910]

როგორც აღინიშნა 1/2010 მოსაზრებაში, ზოგიერთი კრიტერიუმი[11] შესაძლებელია გამოიყენებოდეს დამუშავების კონტროლისთვის. როგორც წესი, არსებობს სიტუაციები, სადაც ღრუბლოვანი სისტემის მომწოდებელი, კონკრეტულ პირობებზე დაყრდნობით, შესაძლებელია განიხილებოდეს მონაცემთა თანა-დამმუშავებლად ან

9 ეს მოსაზრება ფოკუსირებულია დამმუშავებელსა და უფლებამოსილ პირს შორის არსებულ მხოლოდ სისტემურ ურთიერთობაზე.

10 ღრუბლოვანი სისტემის გარემო შესაძლებელია, ასევე, გამოიყენებოდეს ფიზიკური პირების (მომხმარებლების) მიერ აშკარად პირადი მიზნებისთვის. ამ შემთხვევაში, ყურადღებით უნდა გაანალიზდეს აქვს თუ არა ადგილი აღნიშნული პირადი მიზნებისთვის მონაცემთა დამუშავებას, რომელიც გამორიცხავს მომხმარებლის დამმუშავებლად მიჩნევას. თუმცა, ამ საკითხის განხილვა სცდება აღნიშნული მოსაზრების ფარგლებს.

11 მაგ. ინსტრუქციების სიხშირე, ღრუბლოვანი სისტემის მომხმარებლის მიერ მონიტორინგი, მხარეთა ექსპერტიზა.

დამოუკიდებელ დამმუშავებლად, მაგალითად, ეს შესაძლებელია მოხდეს მაშინ, როდესაც მომწოდებელი ამუშავებს მონაცემებს საკუთარი მიზნებიდან გამომდინარე.

აღსანიშნავია, რომ მონაცემთა დამუშავების კომპლექსური გარემოს შემთხვევაშიც კი, სადაც მონაცემთა დამუშავებაში საკუთარი წვლილი სხვადასხვა დამმუშავებელს შეაქვს, მონაცემთა დაცვის წესებთან თანხვედრა და მათი შესაძლო დარღვევისთვის პასუხისმგებლობის განსაზღვრა, ნათლად უნდა განისაზღვროს, რათა თავიდან ავიცილოთ მონაცემთა დაცვის ხარისხის დაცემა ან „კომპეტენციათა ნეგატიური კონფლიქტი," ასევე ჩავარდნები, სადაც დირექტივიდან გამომდინარე ზოგიერთი ვალდებულება ან უფლება მხარეთა მიერ არ არის უზრუნველყოფილი.

ღრუბლოვანი სისტემის არსებული სცენარის თანახმად, მოლაპარაკებებისას, ამ სისტემის მომხმარებლებს შესაძლოა არ ჰქონდეთ თავისუფლება იმ სახელშეკრულებო პირობებთან დაკავშირებით, რომელიც ეხება ღრუბლოვანი სისტემის მომსახურებების გამოყენებას, ვინაიდან ღრუბლოვანი სისტემის ბევრი მომწოდებლისთვის დამახასიათებელია სტანდარტული შეთავაზებები. მიუხედავად ამისა, კონკრეტული მიზნებიდან გამომდინარე, მხოლოდ მომხმარებელმა უნდა

განსაზღვროს დამუშავების ოპერაციების სრული ან ნაწილობრივი განაწილება ღრუბლოვანი სისტემის მომსახურებებზე; ღრუბლოვანი სისტემის მომწოდებლის, როგორც მომხმარებლის წინაშე ხელშემკვრელი მხარის, დანიშნულება, წარმოადგენს მთავარ ფაქტორს ამ ვითარებაში.WP29-ს 1/2010[12] მოსაზრებაში დამმუშავებლისა და უფლებამოსილი პირის ცნების შესახებ აღინიშნა, რომ *„სახელშეკრულებო ბერკეტების დისბალანსი (უფლებრივად) მცირე დამმუშავებელსა და მომსახურების (უფლებრივად) დიდ მომწოდებელს შორის არ უნდა აღიქმებოდეს, როგორც გამამართლებელი პირობა დამმუშავებლისთვის, რათა იგი დაეთანხმოს ხელშეკრულების იმ პირობებსა და წესებს, რომელიც არ არის შესაბამისობაში მონაცემთა დაცვის კანონმდებლობასთან.“* აქედან გამომდინარე, დამმუშავებელმა უნდა აირჩიოს ღრუბლოვანი სისტემის ის მომწოდებელი, რომელიც უზრუნველყოფს შესაბამისობას მონაცემთა დაცვის კანონმდებლობასთან. განსაკუთრებით აღსანიშნავია გასაფორმებელი ხელშეკრულების პირობები – იგი უნდა შეიცავდეს მონაცემთა უსაფრთხოების სტანდარტულ პირობებს, მათ შორის, რომელიც გამოკვეთილია სამუშაო ჯგუფის მიერ 3.4.3 (ტექნიკური და ორგანიზაციული ზომები) და 3.5 პარაგრაფებში (მონაცემთა ტრანსსასაზღვრო

12 მოსაზრება 1/2010 დამმუშავებლისა და უფლებამოსილი პირის ცნების შესახებ - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

გადაცემა), ასევე დამატებით ზომებს, რომელიც მიზანშეწონილია პროცესის ზედმიწევნობისა და ანგარიშვალდებულების უზრუნველსაყოფად (როგორიცაა დამოუკიდებელი აუდიტი და მომწოდებლის სერტიფიცირება – იხ. 4.2 პარაგრაფი).

ღრუბლოვანი სისტემის მომწოდებლებს (როგორც უფლებამოსილ პირებს) გააჩნიათ კონფიდენციალურობის დაცვის ვალდებულება. 95/46/EC დირექტივა ადგენს, რომ: *„პირებმა, რომლებიც მოქმედებენ მონაცემთა დამმუშავებლის ან უფლებამოსილი პირების ზედამხედველობის ქვეშ, მათ შორის, თავად უფლებამოსილმა პირებმა, რომლებსაც წვდომა აქვთ პერსონალურ მონაცემებზე, არ უნდა დაამუშავონ ისინი, დამმუშავებლისგან ინსტრუქციების მიღების გარეშე, გარდა იმ შემთხვევებისა როდესაც მოთხოვნა მომდინარეობს კანონიდან.“* ღრუბლოვანი სისტემის მომწოდებლის მიერ მომსახურებების განხორციელებისას მონაცემებთან წვდომა საფუძვლიანად რეგულირებულია დირექტივის მე-17 მუხლის დანაწესებთან შესაბამისობაში მოყვანის მოთხოვნით – იხ. 3.4.2.

უფლებამოსილმა პირებმა მხედველობაში უნდა მიიღონ ღრუბლოვანი სისტემის განსახილველი ტიპი (საჯარო, პირადი, გაერთიანების ან ჰიბრიდული/ინფრასტრუქტურა როგორც სერვისი,

პროგრამული უზრუნველყოფა როგორც სერვისი ან პლატფორმა როგორც სერვისი [იხ. დანართი ა) წარმოების მოდელები, ბ) მომსახურების მიწოდების მოდელები) და მომხმარებელთან გაფორმებული მომსახურების სახე. უფლებამოსილი პირები ვალდებულნი არიან მიიღონ უსაფრთხოების ზომები, რომელიც თანხვედრაში უნდა იყოს ევროპული კავშირის კანონმდებლობით მოცემულ ანალოგებთან, და რაც ვრცელდება მონაცემთა დამმუშავებლებისა და უფლებამოსილი პირების იურისდიქციაზე. უფლებამოსილი პირები ასევე უნდა უწევდნენ დახმარებას დამმუშავებლებს მონაცემთა სუბიექტის უფლებების უზრუნველყოფის საკითხებში.

3.3.2 ქვე-კონტრაქტორები

ღრუბლოვანი სისტემის მომსახურებები შესაძლებელია მოიცავდეს ხელშემკვრელი მხარეების ჩართვას, რომლებიც მოქმედებენ როგორც უფლებამოსილი პირები. უფლებამოსილი პირებისთვის, ასევე, დამახასიათებელია, ხელშეკრულების საფუძველზე, პროცესში იმ ქვეკონტაქტორების ჩართვა, რომელთაც შემდგომში ექნებათ წვდომა პერსონალურ მონაცემებზე. თუ უფლებამოსილი პირი ხელშეკრულებას აფორმებს ქვეკონტრაქტორთან, ის ვალდებულია მიაწოდოს აღნიშნული ინფორმაცია მომხმარებელს, ქვეკონტრაქტირებული მომსახურებების დეტა-

ლების, არსებული ან პოტენციური ქვეკონტრაქტორის აღწერილობის მითითებით, ასევე იმის გარანტიით, რომ ეს პირი უზრუნველყოფს ღრუბლოვანი სისტემის მომსახურების მომწოდებლის საქმიანობის შესაბამისობას 95/46/EC დირექტივასთან.

ღრუბლოვანი სისტემის მომწოდებელსა და ქვეკონტრაქტორს შორის დადებული ხელშეკრულებით ქვეკონტრაქტორზე უნდა გავრცელდეს ყველა ის ვალდებულება, რომელიც თანხვედრაშია დამმუშავებელსა და უფლებამოსილ პირს შორის არსებულ სახელშეკრულებო პირობებთან. თავის მოსაზრებაში 1/2010 დამმუშავებლისა და უფლებამოსილი პირის ცნების შესახებ, WP29 განიხილავს უფლებამოსილ პირთა სიმრავლის შესაძლებლობას იმ შემთხვევებში, როდესაც უფლებამოსილ პირებს პირდაპირი ურთიერთობა აქვთ დამმუშავებელთან ან მოქმედებენ როგორც ქვეკონტრაქტორები, როდესაც უფლებამოსილი პირები ახდენენ მათზე დავალებული დამუშავების ნაწილის აუთსორსს. *„დირექტივის არც ერთი დანაწესი ორგანიზაციული მიზნებისთვის არ კრძალავს სხვადასხვა პირების ჩართვას, როგორც უფლებამოსილი პირების ან ქვეკონტრაქტორების, ასევე, არც მათ დავალებათა გადანაწილებას. თუმცა, ყველა მათგანი ვალდებულია დაემორჩილოს ინსტრუქციებს, რომელიც გაცემულია*

დამმუშავებლის მიერ დამუშავების პროცესის საწარმოებლად.“[13]

ასეთ შემთხვევებში, დამუშავების პროცესზე ეფექტური კონტროლის უზრუნველყოფისა და პასუხისმგებლობათა სწორი გადანაწილების მიზნით, მონაცემთა დაცვის კანონმდებლობიდან გამომდინარე ვალდებულებები და პასუხისმგებლობები, ნათლად უნდა გამოიკვეთოს და არ გაიფანტოს აუთსორსის ან ქვეკონტრაქტების დროს. მონაცემთა ქვეკონტრაქტის მეშვეობით დამუშავებისას ვალდებულებათა გადანაწილების შესაძლო მოდელი პირველად წარმოდგენილ იქნა კომისიის 2010 წლის 5 დეკემბრის გადაწყვეტილებით მონაცემთა მესამე ქვეყნებისთვის გადაცემის თაობაზე არსებული სტანდარტული სახელშეკრულებო პირობების შესახებ.[14] ამ მოდელით, ქვეუფლებამოსილი პირის ჩართვა ნებადართულია მხოლოდ მონაცემთა დამმუშავებლის წინასწარი წერილობითი თანხმობით და, ასევე, წერილობითი შეთანხმების საფუძველზე, რომლის პირობები უნდა იყოს იმ პირობების ანალოგიური, რაც განსაზღვრულია უფლებამოსილი პირისთვის. თუ ქვეუფლებამოსილი პირი ვერ შეასრულებს თავის ვალდებულებებს მონაცემთა დაცვის

13 იხ. WP169, გვ. 29, მოსაზრება 1/2010 დამმუშავებლისა და უფლებამოსილი პირის ცნების შესახებ (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf).
14 იხ. ხშირად დასმული კითხვები II.5, WP176.

კუთხით, აღნიშნული ხელშეკრულების საფუძველზე ქვეუფლებამოსილი პირის ვალდებულებების შეუსრულებლობის გამო, უფლებამოსილი პირი მთლიანად იქნება პასუხისმგებელი დამმუშავებლის წინაშე. იმისათვის, რათა მოთხოვნილი გარანტიები მონაცემთა ქვედამმუშავებლის მიერ შესრულდეს, ამ სახის პირობა შესაძლოა გამოიყენებოდეს დამმუშავებელსა და ღრუბლოვანი სისტემის მომწოდებელს შორის დადებულ ნებისმიერ ხელშეკრულებაში, როდესაც ამ უკანასკნელს განზრახული აქვს საკუთარი მომსახურების შესრულება ქვეკონტრაქტის საფუძველზე.

მსგავსი საშუალება, რომელიც უზრუნველყოფს მონაცემთა ქვედამუშავებისთვის შესაბამის გადაწყვეტებს, მოცემულია კომისიის მიერ, მონაცემთა დაცვის ძირითადი რეგულაციის შესახებ კანონპროექტის წარდგენისას.[15] უფლებამოსილი პირის ქმედებები უნდა იყოს მოწესრიგებული ხელშეკრულებით ან სხვა სამართლებრივი აქტით, რომელიც ავალდებულებს უფლებამოსილ პირს დამმუშავებლის წინაშე, და, ასევე, ადგენს, რომ სხვა მოთხოვნებთან ერთად, უფლებამოსილ პირს შეუძლია ჩართოს ქვეუფლებამოსილი პირი მხოლოდ დამმუშავებლის წინასწარი თანხმობის

15 ევროპის პარლამენტისა და საბჭოს კანონპროექტი რეგულაციის შესახებ მონაცემთა ავტომატური დამუშავებისა და ამ მონაცემთა თავისუფალი გადაადგილებისას ფიზიკურ პირთა დაცვის თაობაზე, 25.1.2012.

საფუძველზე (კანონპროექტის 26.2 მუხლი).

WP29-ს აზრით, უფლებამოსილ პირს შეუძლია საკუთარი ქმედებების შესრულების დაკისრება ქვეკონტრაქტორისთვის მხოლოდ დამმუშავებლის თანხმობით, რომელიც ძირითადად, გაცემული უნდა იყოს მომსახურების გაწევის დაწყებამდე[16] იმ ვალდებულების თანხლებით, რომ ქვეკონტრაქტორის ნებისმიერი დამატების ან შეცვლის თაობაზე აცნობებს დამმუშავებელს, რაც თავის მხრივ ხდის მას უფლებამოსილს გააპროტესტოს აღნიშნული ცვლილებები ან შეწყვიტოს კონტრაქტი. ღრუბლოვანი სისტემის მომწოდებელს უნდა ჰქონდეს აშკარა ვალდებულება დაასახელოს პროცესში ჩართული ნებისმიერი ქვეკონტრაქტორი. ამასთან, ხელშეკრულება გაფორმებული უნდა იყოს ღრუბლოვანი სისტემის მომწოდებელსა და ქვეკონტრაქტორს შორის, რაც თანხვედრაშია ღრუბლოვანი სისტემის მომწოდებელსა და დამმუშავებელს შორის არსებული ხელშეკრულების პირობებთან. თუ ადგილი ექნება ხელშეკრულების დარღვევას ქვეუფლებამოსილი მხრიდან, დამმუშავებელი უნდა იყოს უფლებამოსილი ისარგებლოს სახელშეკრულებო პირობებით გათვალისწინებული რესურსებით. ეს შესაძლოა მიიღწეოდეს იმ პირობის განმტკიცებით, რომ უფლებამოსილი პირი არის უშუალოდ პასუხის-

16 იხ. ხშირად დასმული შეკითხვები II, 1, WP176, მიღებული 2010 წლის 12 ივლისს.

მგებელი დამმუშავებლის წინაშე ყველა იმ დარღვევისთვის, რომელიც გამოწვეულია მის მიერ ჩართული ქვეკონტრაქტორების მხრიდან, ან დამმუშავებელი გათვალისწინებულ იქნეს როგორც მესამე მხარედ – ბენეფიციარად, უფლებამოსილ პირსა და ქვეკონტრაქტორს შორის ხელმოწერილ ხელშეკრულებებში, ან იმ პირობით, რომ აღნიშნული ხელშეკრულებები ფორმდება მონაცემთა დამმუშავებლისთვის, ამ უკანასკნელის ხელშეკრულების მხარედ ჩართვით.

3.4 მონაცემთა დაცვის მოთხოვნები მომხმარებლისა და მომწოდებლის ურთიერთობაში

3.4.1 შესაბამისობა ძირითად პრინციპებთან

ღრუბლოვან სისტემაში პერსონალურ მონაცემთა დამუშავების კანონიერება დამოკიდებულია ევროპული კავშირის მონაცემთა დაცვის სამართლის ძირითადი პრინციპების დაცვაზე, კერძოდ, გამჭვირვალობა უნდა იყოს უზრუნველყოფილი მონაცემთა სუბიექტის წინაშე, მიზნის კონკრეტულობისა და ლიმიტირების პრინციპი უნდა იქნეს დაცული და პერსონალური მონაცემები უნდა იქნეს წაშლილი მაშინვე, როდესაც მისი შენახვა აღარ არის აუცილებელი. გარდა ამისა, მონაცემთა დაცვისა და უსაფრთხოების ადეკვატური

დონის უზრუნველსაყოფად შესაბამისი ტექნიკური და ორგანიზაციული ზომები უნდა იყოს იმპლემენტირებული.

3.4.1.1 გამჭვირვალობა

გამჭვირვალობა არის უმთავრესი პირობა პერსონალურ მონაცემთა სამართლიანი და კანონიერი დამუშავებისთვის. 95/46/EC დირექტივა ავალდებულებს ღრუბლოვანი სისტემის მომხმარებლებს აცნობონ მონაცემთა სუბიექტს, თუ ვისგან არის მის შესახებ ინფორმაცია შეგროვებული, აცნობონ მისი ვინაობა და დამუშავების მიზანი. ღრუბლოვანი სისტემის მომხმარებელმა, ასევე, უნდა მიაწოდოს დამატებითი ინფორმაცია, როგორიცაა მიმღებების ვინაობისა ან მათი კატეგორიების შესახებ, რაც შესაძლებელია მოიცავდეს უფლებამოსილ და ქვეუფლებამოსილ პირებს. ამ ინფორმაციის მიწოდება წარმოადგენს დამუშავების სამართლიანობის წინაპირობას მონაცემთა სუბიექტის მიმართ (იხ. დირექტივის მე-10 მუხლი).[17]

გამჭვირვალობა უნდა იქნეს უზრუნველყოფილი ღრუბლოვანი სისტემის მომხმარებელს, მომწო-

17 მონაცემთა სუბიექტის ინფორმირებულობის შესახებ შესაბამისი მოვალეობა წარმოიშობა მაშინ, როდესაც მონაცემები არ იქნა შეგროვებული უშუალოდ მონაცემთა სუბიექტისგან, არამედ სხვადასხვა წყაროდან, რომელიც გასაჯაროვებული ან შენახული იქნება მესამე პირისათვის (იხ. მე-11 მუხლი).

დებელსა და ქვეკონტრაქტორებს (ასეთის არსებობის შემთხვევაში) შორის. ღრუბლოვან სისტემაში მომხმარებელს შეუძლია შეაფასოს პერსონალურ მონაცემთა დამუშავების კანონიერება მხოლოდ მაშინ, თუ მომწოდებელი აცნობებს ყველა მნიშვნელოვან საკითხს. დამმუშავებელმა, რომელიც განიხილავს ღრუბლოვანი სისტემის მომწოდებლის ჩართვას პროცესში, გულდასმით უნდა შეამოწმოს მომწოდებლის პირობები და შეაფასოს მონაცემთა დაცვის პერსპექტივიდან გამომდინარე.

ღრუბლოვან სისტემაში გამჭვირვალობა ნიშნავს, რომ ღრუბლოვანი სისტემის მომხმარებელი ინფორმირებულია ყველა ქვეკონტრაქტორის შესახებ, რომლებსაც წვლილი შეაქვთ ღრუბლოვანი სისტემის მომსახურებების განხორციელებაში და, ასევე, ინფორმაცია არსებობს ყველა იმ ადგილმდებარეობის შესახებ, სადაც შესაძლოა დამუშავდეს პერსონალური მონაცემები.[18]

თუ მომსახურების ფუნქციონირება ითვალისწინებს ღრუბლოვანი სისტემის მომხმარებლის სისტემაზე პროგრამული მხარდაჭერის ინსტალირებას (მაგ. ბროუზერის მოდიფიკაციები) საუკეთე-

18 მხოლოდ ამ შემთხვევაში შეეძლება მას შეაფასოს საკითხი თუ რამდენად არის შესაძლებელი მონაცემთა გადაცემა ე.წ. მესამე ქვეყნებისადმი EEA-ს ფარგლებს გარეთ, რომლებიც არ ადგენენ მონაცემთა დაცვის ადეკვატურ დონეს 95/46/EC დირექტივის შესაბამისად. იხ. ასევე 3.4.6 პარაგრაფი.

სო მაგალითის უზრუნველსაყოფად, ღრუბლოვანი სისტემის მომწოდებელმა უნდა მოახდინოს მომხმარებლის ინფორმირება ამის შესახებ, კერძოდ, თავისებურებების კუთხით მონაცემთა დაცვისა და მათი უსაფრთხოების პერსპექტივიდან გამომდინარე. ასევე პირიქით, ღრუბლოვანი სისტემის მომხმარებელს შეუძლია დასვას ეს საკითხი წინასწარ, თუ აღნიშნული არ არის საკმარისად მიმოხილული ღრუბლოვანი სისტემის მომწოდებლის მიერ.

3.4.1.2 მიზნის კონკრეტულობა და ლიმიტირება

მიზნის კონკრეტულობისა და ლიმიტირების პრინციპი მოითხოვს, რომ პერსონალური მონაცემები შეგროვდეს განსაზღვრული, მკაფიო, კანონიერი მიზნებისთვის და არ დამუშავდეს თუ ეწინააღმდეგება შეგროვების მიზნებს (იხ. 95/46/EC დირექტივის მე-6 მუხლი -b- ქვეპუნქტი). სუბიექტებისგან პერსონალურ მონაცემთა შეგროვებამდე, ღრუბლოვანი სისტემის მომხმარებელმა უნდა განსაზღვროს დამუშავების მიზანი (მიზნები) და აცნობოს ამის თაობაზე მონაცემთა სუბიექტს. ღრუბლოვანი სისტემის მომწოდებელმა არ უნდა დაამუშავოს პერსონალური მონაცემები იმ მიზნებისთვის, რომლებიც არ არის თანხვედრაში თავდაპირველ მიზანთან.

გარდა ამისა, უნდა იქნეს უზრუნველყოფილი ისიც, რომ პერსონალური მონაცემები ღრუბლოვანი სისტემის მომწოდებლის ან ქვეკონტრაქტორის მიერ არ იყოს დამუშავებული (უკანონოდ) სხვა მიზნებისთვის. ჩვეულებრივი ღრუბლოვანი სისტემა შესაძლებელია მარტივად მოიცავდეს ქვეკონტრაქტორთა დიდ რიცხვს, შესაბამისად, პერსონალურ მონაცემთა დამუშავების რისკი სხვა, თანხვედრაში არმყოფი მიზნებისთვის, მაღალი ალბათობისაა. რისკების მინიმუმანდე დასაყვანად, ღრუბლოვანი სისტემის მომწოდებელსა და მომხმარებელს შორის გაფორმებული ხელშეკრულება უნდა მოიცავდეს ტექნიკურ და ორგანიზაციულ ზომებს, რომელიც ამცირებს რისკს და უზრუნველყოფს გარანტიებს, რის შესაბამისად შესაძლებელი იქნება ღრუბლოვანი სისტემის დასაქმებულების ან ქვეკონტრაქტორების მიერ პერსონალურ მონაცემთა დამუშავების პროცესის ჩაწერა და შემოწმება.[19] ჯარიმები უნდა განისაზღვროს ხელშეკრულებით მომწოდებლის ან ქვეკონტრაქტორის წინააღმდეგ, თუ მონაცემთა დაცვის კანონმდებლობა დარღვეულია.

3.4.1.3 მონაცემთა წაშლა

95/46/EC დირექტივის მე-6 მუხლის -e- ქვეპუნქტით, პერსონალური მონაცემები უნდა იქნეს შენახული მონაცემთა სუბიექტების იდენტიფიცრე-

19 იხ. 3.4.3.

ბადი ფორმით იქამდე სანამ ეს აუცილებელია იმ მიზნის მისაღწევად, რისთვისაც შეგროვდა მონაცემები ან თუ ხდება მათი შემდგომი დამუშავება. ის პერსონალური მონაცემები, რომელიც აღარ არის საჭირო უნდა წაიშალოს ან სრულად ანონიმირდეს. თუ ამგვარი მონაცემის წაშლა დაუშვებელია შენახვის საკნონმდებლო მოთხოვნიდან გამომდინარე (მაგ. საგადასახადო რეგულაციები), აღნიშნულ პერსონალურ მონაცემებთან წვდომა უნდა დაიბლოკოს. ღრუბლოვანი სისტემის მომხმარებლის ვალდებულებას წარმოადგენს ის, რომ უზრუნველყოს პერსონალური მონაცემების წაშლა მაშინვე, როდესაც ისინი აღარ არის საჭირო ზემოაღნიშნული გარემოებების შემთხვევაში.[20]

მონაცემთა წაშლის პრინციპი ვრცელდება ნებისმიერ პერსონალურ მონაცემზე, მიუხედავად მათი შენახვის ფორმისა მყარ დისკებსა თუ სხვა მატარებლებზე (მაგ. სარეზერვო ფირზე). რამდენადაც პერსონალური მონაცემები შესაძლოა შენახულ იქნეს ჭარბად სხვადასხვა სერვერებსა და ადგილას, აუცილებელია თითოეული ნაწილის წაშლა აღდგენის შესაძლებლობის გამორიცხვით (მაგ. წინა ვერსიები, დროებითი ფაილები და, ასევე, ფაილის ფრაგმენტებიც უნდა წაიშალოს).

20 მონაცემთა წაშლის საკითხი წარმოადგენს როგორც ღრუბლოვან სისტემასთან დაკავშირებული ხელშეკრულების მოქმედებისას მოსაწესრიგებელ საკითხს, ისე აღნიშნული შეთანხმების შეწყვეტისას – პირობას. ეს ასევე საყურადღებოა ქვე-კონტრაქტორის ჩანაცვლების ან გასვლის შემთხვევაშიც.

ღრუბლოვანი სისტემის მომხმარებლები უნდა იყვნენ ინფორმირებულები ქმედების განხორციელების შესახებ. მონაცემები,[21] რომელიც აადვილებს შენახვის, მოდიფიკაციის ან წაშლის შემოწმებას, შესაძლოა მოიცავდეს იმ პირის პერსონალურ მონაცემებს, რომელმაც მოახდინა აღნიშნული პროცესის ინიცირება.[22]

პერსონალურ მონაცემთა უსაფრთხო წაშლა მოითხოვს შენახვის მოწყობილობის განადგურებას, დემაგნიტიზირებას ან პერსონალურ მონაცემთა წაშლას ზემოდან გადაწერის მეთოდით. პერსონალურ მონაცემთა ზემოდან გადაწერისთვის სპეციალური პროგრამული საშუალებები უნდა გამოიყენებოდეს, რომელიც გადააწერს მონაცემებს მრავალჯერ და შესაბამისი სიზუსტით.

ღრუბლოვანი სისტემის მომხმარებელი უნდა დარწმუნდეს, რომ ზემოხსენებული შემთხვევებისთვის ღრუბლოვანი სისტემის მომწოდებელი უზრუნველყოფს დაცულ წაშლას და, ასევე, იმას, რომ ხელშეკრულება მომხმარებელსა და მომწოდებელს შორის შეიცავდეს პერსონალურ მონაცემთა წაშლასთან დაკავშირებით აშკარა დებულებებს.[23] იგივე ეხება ღრუბლოვანი სისტემის

21 შენიშვნები შენახვის მოთხოვნებთან დაკავშირებით არის მოცემული 4.3.4.2-ით.
22 ეს ნიშნავს, რომ შენახვის ფაილების შენახვის ვადა უნდა იქნას განსაზღვრული და ის პროცესები, რომლებიც უზრუნველყოფს წაშლასა და ანონიმიზაციას არის სახეზე.
23 იხ. 3.4.3.

მომწოდებელსა და ქვეკონტრაქტორს შორის დადებულ ხელშეკრულებებს.

3.4.2 სახელშეკრულებო უსაფრთხოების ზომები დამმუშავებლისა და უფლებამოსილი პირის ურთიერთობ(ებ)ისას

თუ დამმუშავებლები გადაწყვეტენ გააფორმონ ღრუბლოვანი სისტემის მომსახურებების შესახებ ხელშეკრულება, მათ ევალებათ აირჩიონ ის უფლებამოსილი პირი, რომელიც უზრუნველყოფს უსაფრთხოების შესაბამისი ტექნიკური და ორგანიზაციული ზომების ფუნქციონირებას, რაც გავრცელდება დამუშავების პროცესზე და იქნება მასთან შესაბამისობაში (95/46/EC დირექტივის მე-17(2) მუხლი). მეტიც, ისინი ვალდებულნი არიან გააფორმონ ხელშეკრულება ღრუბლოვანი სისტემის მომწოდებელთან, რაც აღნიშნულია 95/46/EC დირექტივის მე-17(3) მუხლით. ეს მუხლი განსაზღვრავს მოთხოვნას, რომლის თანახმად უნდა არსებობდეს ხელშეკრულება ან სხვა სავალდებულო დოკუმენტი, რომელიც გავრცელდება დამმუშავებელსა და უფლებამოსილ პირს შორის არსებულ ურთიერთობაზე. მტკიცების მიზნისთვის, ხელშეკრულების ნაწილები ან სამართლებრივი აქტი, რომელიც ეხება მონაცემთა დაცვას, ასევე, ტექნიკური და ორგანიზაციული უსაფრთხოების მოთხოვნებს, უნდა იყოს გაფორმებული წერილობით ან სხვა ექვივალენტური ფორმით.

ხელშეკრულება უნდა განსაზღვრავდეს იმ ვალდებულებას მაინც, რომ უფლებამოსილი პირი ასრულებდეს დამმუშავებლის მიერ გაცემულ ინსტრუქციებს და დანერგოს ტექნიკური და ორგანიზაციული ზომები პერსონალური მონაცემების ადეკვატურად დაცვისთვის. სამართლებრივი სიზუსტის უზრუნველსაყოფად ხელშეკრულება ყურადღებას უნდა ამახვილებდეს შემდეგ საკითხებზე:

1. მომხმარებლის მიერ გაცემული ინსტრუქციების დეტალები (ფარგლები და მოდელები), მომსახურების სახეობასთან მიმართებით (რომელიც უნდა იყოს მიზნობრივი და გაზომვადი) და შესაბამისი სანქციები (ფინანსური ან სხვაგვარი, რომელიც მოიცავს მომწოდებლის წინააღმდეგ სარჩელის შეტანის შესაძლებლობას დარღვევის შემთხვევაში).
2. უსაფრთხოების ზომების განსაზღვრა. ეს უნდა შეასრულოს ღრუბლოვანი სისტემის მწარმოებელმა იმ რისკებიდან გამომდინარე, რაც ახლავს დამუშავებას და იმ მონაცემთა ბუნების გათვალისწინებით, რაც უნდა იქნეს დაცული. უმნიშვნელოვანესია, რომ კონკრეტული ტექნიკური და ორგანიზაციული ზომები განისაზღვროს 3.4.3 პარაგრაფის მიხედვით. აღნიშნული არ კრძალავს მეტად მკაცრი ზომების გამოყენებას, რომელიც შეიძლება იქნეს გათვალისწნებული მომხმარებლის ქვეყნის კანონმდებლობით.

3. ღრუბლოვანი მომსახურების შინაარსი და მიწოდების დრო უნდა განისაზღვროს ღრუბლოვანი სისტემის მომწოდებლის მიერ, ხოლო დამუშავების ფარგლები, ხასიათი და მიზანი, ასევე, დასამუშავებელი პერსონალური მონაცემები უნდა განისაზღვროს დამმუშავებლის მიერ.

4. პირობები, რომელიც ეხება პერსონალურ მონაცემთა დაბრუნებას ან განადგურებას უნდა იყოს დაკონკრეტებული. მეტიც, უნდა იყოს უზრუნველყოფილი პერსონალურ მონაცემთა უსაფრთხო წაშლა ღრუბლოვანი სისტემის მომხმარებლის მოთხოვნის საფუძველზე.

5. კონფიდენციალურობის პირობის ჩართვა, რომელიც ავალდებულებს ღრუბლოვანი სისტემის მომწოდებელს და მის ნებისმიერ დასაქმებულს, რომელსაც შესაძლოა ჰქონდეს წვდომა პერსონალურ მონაცემებზე. მხოლოდ ავტორიზებულ პირებს შეუძლიათ ჰქონდეთ წვდომა პერსონალურ მონაცემებზე.

6. მომწოდებლის ვალდებულება, გაუადვილოს მომხმარებელს მონაცემთა სუბიექტების უფლების რეალიზაცია, როგორიცაა წვდომა, შესწორება ან წაშლა.

7. ხელშეკრულება ნათლად უნდა ადგენდეს, რომ ღრუბლოვანი სისტემის მწარმოებელმა არ უნდა მიაწოდოს მონაცემები მესამე პირებს, შენახვის მიზნითაც კი, გარდა იმ შემთხვევისა, თუ ხელშეკრულება ითვალისწინებს აღნიშნულს ქვეკონ-

ტრაქტორებისთვის. ხელშეკრულება უნდა ადგენდეს, რომ ქვეკონტრაქტორები უნდა მოქმედებდნენ დამმუშავებლის მიერ მიღებული თანხმობის შემთხვევაში და უფლებამოსილი პირის იმ ვალდებულებით, რომ შეატყობინოს დამმუშავებელს ნებისმიერი ცვლილება, რა დროსაც ეს უკანასკნელი იტოვებს შესაძლებლობას გააპროტესტოს აღნიშნული ცვლილებები ან შეწყვიტოს ხელშეკრულება. ღრუბლოვანი სისტემის მომწოდებელი უნდა იყოს ვალდებული დაასახელოს ყველა ქვეკონტრაქტორი, რომელიც ჩართულია პროცესში (მაგ. საჯარო ციფრული რეესტრი). უნდა იყოს უზრუნველყოფილი ღრუბლოვანი სისტემის მომწოდებელსა და ქვეკონტრაქტორს შორის არსებული ხელშეკრულების შესაბამისობა იმ ხელშეკრულების დებულებებთან, რომელიც გაფორმებულია ღრუბლოვანი სისტემის მომწოდებელსა და მომხმარებელს შორის (მაგ. ქვეკონტრაქტორებს აქვთ იგივე სახელშეკრულებო ვალდებულებები დამმუშავებლის წინაშე, რაც ღრუბლოვანი სისტემის მომწოდებლებს). კერძოდ, უნდა იყოს გარანტირებული, რომ ღრუბლოვანი სისტემის მომწოდებელი და ყველა ქვეკონტრაქტორი მოქმედებდნენ მხოლოდ ღრუბლოვანი სისტემის მომხმარებლისგან მიღებული ინსტრუქციების შესაბამისად. როგორც ქვეუფლებამოსილი პირის შესახებ არსებულ პარაგრაფში აღინიშნა, ვალდებულებათა ჯაჭვი ხელშეკრულებით ნათლად

უნდა იყოს განსაზღვრული. იგი უნდა ადგენდეს ვალდებულებას უფლებამოსილი პირისათვის, რომელიც მოიცავს საერთაშორისო გადაცემებს, მაგალითად, ქვეკონტრაქტორებთან ხელშეკრულებების გაფორმება 2010/87/EU ხელშეკრულების სტანდარტული პირობების საფუძველზე.

8. ღრუბლოვანი სისტემის მომწოდებლის პასუხისმგებლობის დადგენა, რომელიც ეხება ღრუბლოვანი სისტემის მომხმარებლის შეტყობინებას იმ შემთხვევაში, თუკი ადგილი ექნება მონაცემთა დაცვის დარღვევას, რაც, თავის მხრივ, გავლენას ახდენს ღრუბლოვანი სისტემის მომხმარებლის მონაცემებზე.

9. ღრუბლოვანი სისტემის მომწოდებლის ვალდებულება შეადგინოს იმ ადგილმდებარეობის სია, სადაც შესაძლებელია დამუშავდეს მონაცემები.

10. დამმუშავებლის უფლებები – გაუწიოს მონიტორინგი და ღრუბლოვანი სისტემის მომწოდებლის საპასუხო ვალდებულება – ითანამშრომლოს მასთან.

11. ხელშეკრულებით უნდა იყოს დადგენილი, რომ ღრუბლოვანი სისტემის მომწოდებელი ვალდებულია მოახდინოს მომხმარებლის ინფორმირება შესაბამისი ცვლილებების თაობაზე, რომელიც ეხება ღრუბლოვანი სისტემის მომსახურებებს, როგორიცაა დამატებითი ფუნქციების ჩართვა.

12. ხელშეკრულება უნდა ითვალისწინებდეს ღრუბლოვანი სისტემის მომწოდებლის ან ქვეკონ-

ტრაქტორების მიერ წარმოებული პერსონალური მონაცემების დამუშავების პროცესის შენახვასა და შემოწმებას.

13. კანონის აღმასრულებელი ორგანოების მიერ ღრუბლოვანი სისტემის მომხმარებლის შეტყობინება ნებისმიერი სავალდებულო მოთხოვნის შესახებ, რომელიც ეხება პერსონალურ მონაცემთა გაცემას, რაც სხვა შემთხვევაში დაუშვებელია, მაგალითად, აკრძალვა სისხლის სამართლის კანონმდებლობის შესაბამისად, რათა დაცულ იქნეს გამოძიების საიდუმლოობა.

14. მომწოდებლის ძირითადი ვალდებულება, უზრუნველყოს გარანტიები მონაცემთა დამუშავების შიდაორგანიზაციული პროცესების (ქვეკონტრაქტორის მიერ წარმოებული პროცესების, არსებობის შემთხვევაში) შესაბამისობა ეროვნულ და საერთაშორისო სამართლებრივ მოთხოვნებსა და სტანდარტებთან.

დამმუშავებლის მხრიდან დარღვევის შემთხვევაში, ნებისმიერი პირს, რომელსაც მიადგა ზიანი უკანონო დამუშავების შედეგად, უნდა ჰქონდეს შესაძლებლობა მიიღოს კომპენსაცია დამმუშავებლისგან მიყენებული ზიანის გამო. იმ შემთხვევაში, თუ უფლებამოსილი პირები გამოიყენებენ მონაცემებს სხვა მიზნისთვის, ან გასცემენ მას იმ სახით, რაც დაარღვევს ხელშეკრულებას, ისინი ჩაითვლებიან დამმუშავებლებად და იქნებიან

ვალდებულნი იმ ზიანისთვის, რაც დადგა მათი ბრალეული ქმედების ფარგლებში.

უნდა აღინიშნოს, რომ ბევრ შემთხვევაში, ღრუბლოვანი სისტემის მომწოდებლები სთავაზობენ დამმუშავებლებს მომსახურების სტანდარტულ პირობებს და ხელშეკრულების გაფორმებას, რომელიც წინ წამოწევს პერსონალურ მონაცემთა დამუშავების სტანდარტულ ფორმატს. სახელშეკრულებო ბერკეტების დისბალანსი (უფლებრივად) მცირე დამმუშავებელსა და მომსახურების (უფლებრივად) დიდ მომწოდებელს შორის არ უნდა აღიქმებოდეს, როგორც გამამართლებელი პირობა დამმუშავებლისთვის, რათა იგი დაეთანხმოს ხელშეკრულების იმ პირობებსა და წესებს, რომელიც არ არის შესაბამისობაში მონაცემთა დაცვის კანონმდებლობასთან.

3.4.3 მონაცემთა დაცვისა და უსაფრთხოების ტექნიკური და ორგანიზაციული ზომები

95/46/EC დირექტივის მე-17(2) მუხლი აკისრებს მთელ პასუხისმგებლობას ღრუბლოვანი სისტემის მომხმარებლებს (რომელიც მოქმედებენ, როგორც მონაცემთა დამმუშავებლები), აირჩიონ ისეთი ღრუბლოვანი სისტემის მომწოდებლები, რომლებიც ახდენენ მონაცემთა უსაფრთხოების ტექნიკური და ორგანიზაციული ზომების იმპლემენტირებას, რათა დაიცვან პერსონალური მონა-

ცემები და იყვნენ ანგარიშვალდებულები.

უსაფრთხოების ისეთ ძირითად მიზნებთან ერთად, როგორიცაა ხელმისაწვდომობა, კონფიდენციალურობა და ნამდვილობა, ყურადღება, ასევე, უნდა გამახვილდეს მონაცემთა დაცვის თანმდევ მიზნებზე, როგორიცაა გამჭვირვალობა (იხ. 3.4.1.1), განცალკევება,[24] ჩარევაუნარიანობა, ანგარიშვალდებულება და პორტატულობა. ეს ნაწილი ხაზს უსვამს მონაცემთა დაცვის ცენტრალურ მიზნებს, რაც არ კრძალავს სხვა, უსაფრთხოებიდან გამომდინარე რისკების დამუშავებისთვის დამატებითი ღრონისძიებების დანერგვას.[25]

3.4.3.1 ხელმისაწვდომობა

ხელმისაწვდომობის არსებობა ნიშნავს პერსონალურ მონაცემებთან დროულ და საიმედო წვდომის უზრუნველყოფას.

ღრუბლოვან სისტემაში ხელმისაწვდომობისთვის ერთ-ერთ ზიანის მომტანს წარმოადგენს ღრუბლოვანი სისტემის მომხმარებელსა და მომწოდებელს შორის არსებული ქსელური კავშირის ან სერვერის მუშაობის შემთხვევითი შეწყვეტა, რო-

24 გერმანიაში, „დაუკავშირებლობის“ განვრცობილი ცნება წამოყენებულ იქნა კანონმდებლობით და მხარდაჭერილია მონაცემთა დაცვის კომისართა კონფერენციის მიერ.
25 იხ. მაგ. ENISA ხელმისაწვდომია http://www.enisa.europa.eu/activities/risk-managment/files/deliverables/cloud-computing-risk-assessment.

მელიც გამოწვეულია ისეთი სახიფათო შეტევებით, როგორიცაა (მიწოდებული) მომსახურების უარყოფის (DoS)[26] შეტევა. ხელმისაწვდომობის სხვა რისკ-ფაქტორები მოიცავს მოწყობილობის შემთხვევით მწყობრიდან გამოსვლას, როგორც ქსელში, ისე ღრუბლოვან სისტემაში დამუშავებისას, ასევე, მონაცემთა შენახვის სისტემის, კვების მწყობრიდან გამოსვლასა და სხვა ინფრასტრუქტურულ პრობლემებს.

მონაცემთა დამმუშავებელმა უნდა გადაამოწმოს არის თუ არა მიღებული ღრუბლოვანი სისტემის მომწოდებლების მიერ შესაბამისი ზომები, როგორიცაა სარეზერვო ინტერნეტ-ბმულების არსებობა, შენახვის საკმაო ადგილი და მონაცემთა რეზერვაციის ეფექტური მექანიზმები, რომელიც სათანადო წინააღმდეგობას უწევს დარღვევის შესაძლო რისკებს.

3.4.3.2 ნამდვილობა

ნამდვილობა შესაძლებელია განისაზღვროს, როგორც კონდიცია, როდესაც მონაცემები არის ნამდვილი და არ არის განზრახ ან შემთხვევით

26 DoS შეტევა წარმოადგენს გააზრებულ მცდელობას იმისა, რომ კომპიუტერული ან ქსელური რესურსი გახდეს ხელმიუწვდომელი ავტორიზებული მომხმარებლებისთვის, დროებით ან განუსაზღვრელი ვადით (მაგ. შეტევის სისტემეთა დიდი რაოდენობით, რომელიც პარალიზებას უწევს მიზანს გარე კომუნიკაციის უამრავი მოთხოვნის მეშვეობით).

შეცვლილი დამუშავების, შენახვის ან გადაცემის დროს. ნამდვილობის ცნება შესაძლებელია გავრცელდეს IT სისტემებზე, რაც მოითხოვს პერსონალურ მონაცემთა უცვლელად დამუშავებას ამ სისტემების მეშვეობით.

პერსონალური მონაცემების მიმართ ცვლილებების აღმოჩენა შესაძლებელია მოხდეს კრიპტოგრაფირებული ნამდვილობის დადგენის მექანიზმებით, როგორიცაა ნამდვილობის შესახებ კოდების შეტყობინება ან გასაღების სისტემა.

ღრუბლოვან სისტემაში IT სისტემის ნამდვილობის დარღვევა შესაძლოა თავიდან იქნეს აცილებული ჩარევის დეტექციის/პრევენციული სისტემების (IPS/IDS) საშუალებით. ეს მნიშვნელოვანია ღია ტიპის ქსელის პირობებში, სადაც ღრუბლოვანი სისტემები ჩვეულებრივ ფუნქციონირებენ.

3.4.3.3 კონფდენციალურობა

ღრუბლოვანი სისტემის გარემოში, კრიპტაცია მნიშვნელოვან როლს თამაშობს პერსონალურ მონაცემთა კონფიდენციალურობის დაცვაში, თუ იგი იქნება სწორედ იმპლემენტირებული, თუმცა ეს ვერ უზრუნველყოფს პერსონალურ მონაცემთა შეუქცევად ანონიმირებას.[27] პერსონალურ

27 95/46/EC დირექტივის პრეამბულის 26-ე აბზაცი: „(...); დაცვის პრინციპები არ ვრცელდება იმ მონაცემებზე, რომელიც არის ანონიმირებული, იმგვარად, როდესაც ვერ ხერხდება მონაცემ-

მონაცემთა კრიპტაცია უნდა გამოიყენებოდეს ნებისმიერ შემთხვევაში, როდესაც ხდება მათი ტრანზიტი ან ისინი ხელმისაწვდომია უმოქმედო მდგომარეობაში.[28] ზოგიერთ შემთხვევაში, (მაგ. IaaS შენახვის სერვისი) ღრუბლოვანი სისტემის მომხმარებელი შესაძლოა არ დაკმაყოფილდეს ღრუბლოვანი სისტემის მომწოდებლის კრიპტაციის მეთოდით და მოახდინოს მათი კრიპტაცია ღრუბლოვან სისტემაში მონაცემთა განთავსებამდე. უმოქმედო მდგომარეობაში არსებული მონაცემები მოითხოვს განსაკუთრებულ ყურადღებას კრიპტაციის გასაღების სისტემაზე, რამდენადაც მონაცემთა უსაფრთხოება განსაკუთრებულად დამოკიდებული ხდება კრიპტაციის გასაღებთა კონფიდენციალურობაზე.

ღრუბლოვანი სისტემის მომწოდებელს, მომხმარებელსა და მონაცემთა ცენტრებს შორის კომუნიკაცია უნდა იყოს დაშტრიხული. ღრუბლოვანი

თა სუბიექტის იდენტიფიცირება, (...)." იმავე მხრივ, მონაცემთა ტექნიკური ფრაგმენტაცია, რომელიც შესაძლებელია გამოიყენებოდეს ღრუბლოვანი სისტემის მომსახურების იმპლემენტირებისთვის, რის მიხედვითაც არ ხდება მონაცემთა შეუქცევადი ანონიმირება, არ გულისხმობს, რომ მათზე არ ვრცელდება მონაცემთა დაცვის წესები.

28 იგივე შეიძლება ითქვას მონაცემთა დამმუშავებლების მიმართ, რომლებიც გეგმავენ 95/46/EC დირექტივის მე-8 მუხლით განსაზღვრული განსაკუთარებული კატეგორიის მონაცემთა (მაგ. ჯანმრთელობის მდგომარეობის შესახებ) გადაცემას ღრუბლოვანი სისტემისთვის, რომლებსაც, თავის მხრივ, აქვთ კონფიდენციალურობის განსაზღვრული სამართლებრივი ვალდებულება.

ფლატფორმის დისტანციური ადმინისტრირება უნდა მიმდინარეობდეს მხოლოდ კომუნიკაციის დაცული ქსელის საშუალებით. თუ მომხმარებელი გეგმავს არამარტო შენახვას, არამედ პერსონალურ მონაცემთა შემდგომ დამუშავებას ღრუბლოვან სისტემაში (მაგ. მონაცემთა ჩანაწერების ბაზების მოძიებას), მან უნდა გააცნობიეროს, რომ მონაცემთა კრიპტაცია შეუძლებელია მონაცემთა დამუშავებისას (გარდა ძალზედ სპეციფიკური ოპერაციების შემთხვევაში).

ტექნიკური ზომები, რომელიც მიზნად ისახავს კონფიდენციალურობის დაცვას, მოიცავს ავტორიზაციის მექანიზმებს და ნამდვილობის დადგენის ეფექტურ მეთოდებს (მაგ. ნამდვილობის ორმხრივი დადგენა). ხელშეკრულების პირობები, ასევე, უნდა ადგენდეს კონფიდენციალურობის ვალდებულებებს ღრუბლოვანი სისტემის მომხმარებლის, მომწოდებლისა და ქვეკონტრაქტორთან დასაქმებული პირებისთვის.

3.4.3.4 გამჭვირვალობა

ტექნიკური და ორგანიზაციული ზომები უნდა განამტკიცებდნენ გამჭვირვალობას, მათი გადახედვის შესაძლებლობის უზრუნველსაყოფად, იხ. 3.4.1.1.

3.4.3.5 განცალკევება (მიზნის ლიმიტირება)

ღრუბლოვან გარემოში, ისეთი რესურსები, როგორიცაა შემნახველი ადგილები, მეხსიერება და ქსელი გაზიარებულია ბევრ დამქირავებელზე. აღნიშნული წარმოქმნის მონაცემთა გასაჯაროვებისა და არალეგიტუმური მიზნებისთვის დამუშავების ახალ რისკებს. „განცალკევება," როგორც დაცვის მიზანი განკუთვნილია იმისათვის, რათა გაამახვილოს საკითხისადმი ყურადღება და წვილილი შეიტანოს იმის უზრუნველყოფაში, რომ მონაცემები არ გამოიყენებოდეს საწყისი მიზნების გვერდის ავლით (95/46/EC დირექტივის მე-6 მუხლის -b- ქვეპუნქტი), ასევე უზრუნველყოს კონფიდენციალურობა და ნამდვილობა.[29]

განცალკევების მიღწევა, პირველ რიგში, მოითხოვს იმ უფლებამოსილებების შესაბამის მენეჯმენტს და რეგულარულ გადახედვას, რომელიც ეხება პერსონალურ მონაცემთა წვდომას. უფლებამოსილებების განაწილება განსაკუთრებული პრივილეგიების მინიჭებით თავიდან უნდა ავიცილოთ (მაგ. არც მომხმარებელი და არც ადმინისტრატორი არ უნდა იყოს უფლებამოსილი ღრუბლოვანი სისტემის სრულ წვდომაზე). უფრო ზუსტად, ადმინისტრატორები და მომხმარებლები უფლებამოსილნი უნდა იყვნენ მოახდინონ წვდომა მხოლოდ იმ ინფორმაციაზე, რომელიც

29 იხ. 3.4.1.2.

აუცილებელია მათი ლეგიტიმური მიზნებისთვის (მინიმალური პრივილეგიის პრინციპი).

მეორე მხრივ, თუკი ფიზიკური რესურსების განაწილებისთვის სხვადასხვა ღრუბლოვანი სისტემის მომხმარებლებს შორის გამოიყენება ვირტუალური საშუალებები, განცალკევება დამოკიდებულია ტექნიკურ ზომებზეც, როგორიცაა ზედამხედველობის გამყარება და გაზიარებული რესურსების სწორი მენეჯმენტი.

3.4.3.6 ჩარევაუნარიანობა

95/46/EC დირექტივა მონაცემთა სუბიექტებს ანიჭებს წვდომის, შესწორების, წაშლის, დაბლოკვისა და გასაჩივრების უფლებებს (იხ. მე-12 და მე-14 მუხლები). ღრუბლოვანი სისტემის მომხმარებელი უნდა დარწმუნდეს, რომ მომწოდებელი არ ადგენს წინაღობებს ტექნიკური და ორგანიზაციული ზომების რეალიზაციისთვის, მათ შორის იმ შემთხვევებშიც, როდესაც მონაცემები შემდგომში მუშავდება ქვეკონტრაქტორების მიერ.

მომხმარებელსა და მომწოდებელს შორის ხელშეკრულება უნდა ადგენდეს, რომ ღრუბლოვანი სისტემის მომწოდებელი ვალდებულია მხარდაჭერა გაუწიოს მომხმარებელს მონაცემთა სუბიექტების უფლებების რეალიზაციის გამარტივებისთვის და უზრუნველყოს იგივე პირობა ქვეკონტრა-

ქტორებისთვის.[30]

3.4.3.7 გადატანაუნარიანობა

ამჟამად, ღრუბლოვანი სისტემის მომწოდებელთა უმარავლესობა არ იყენებს მონაცემთა ისეთ სტანდარტულ ფორმატებსა და მომსახურებების ფორმებს, რომელიც ხელს უწყობს შეთავსებადობასა და გადატანაუნარიანობას სხვადასხვა ღრუბლოვანი სისტემის მომწოდებელს შორის. თუ ღრუბლოვანი სისტემის მომწოდებელი გადაწყვეტს განახორციელოს მიგრაცია ერთი ღრუბლოვანი სისტემის მწარმოებლიდან მეორეზე, გადატანაუნაირანობის ნაკლებობა შესაძლებელია გახდეს ღრუბლოვანი სისტემის მომხმარებლის პერსონალური მონაცემის გადატანის შეუძლებლობის მიზეზი ან წარმოქმნას სირთულეები ახალი ღრუბლოვანი სისტემის მომწოდებლისთვის (ე.წ. მომწოდებელზე მიბმა). იგივე შეიძლება ითქვას მომსახურებებზე, რომელიც მომხმარებელმა შექმნა პირველადი ღრუბლოვანი სისტემის მომწოდებლის მიერ შემოთავაზებულ პლატფორმაზე (პლატფორმა როგორც მომსახურება). სანამ მომხმარებელი აირჩევს ღრუბლოვან მომსახურებას, მან ასევე უნდა შეამოწმოს, თუ როგორ უზრუნველყოფს მომწოდებელი მონაცემთა

30 იხ. ნაწილი 3.4.5 .7. მომწოდებელი ასევე შესაძლოა იქნას დავალებული, მოახდინოს მომხმარებლისთვის რეაგირება მოთხოვნებზე.

გადატანაუნარიანობას.[31]

3.4.3.8 ანგარიშვალდებულება

IT სფეროში ანგარიშვალდებულება შესაძლებელია განიმარტოს როგორც უნარი, დადგინდეს ქმედებები, რომელიც განხორციელებულია დროის კონკრეტულ მომენტში, წარსულსა ან აწმყოში. მონაცემთა დაცვის სფეროში, იგი ყოველთვის იძენს ფართო გაგებას და განიმარტება, როგორც მხარეთა შესაძლებლობა მოახდინონ მონაცემთა დამუშავების პრინციპების იმპლემენტირებისთვის მიღებული შესაბამისი ნაბიჯების დემონსტრირება.

IT ანგარიშვალდებულება მნიშვნელოვანია პერსონალურ მონაცმთა დარღვევების გამოძიებისთვის, სადაც ღრუბლოვანი სისტემის მომხმარებლები, მომწოდებლები და ქვეკონტრაქტორები შესაძლოა იზიარებდნენ ოპერაციულ პასუხისმგებლობებს. ღრუბლოვანი სისტემის პლატფორმის შესაძლებლობა – აწარმოოოს სარწმუნო მონიტორინგი და შენახვის სრულყოფილი მექანიზმები, უპირველესი მნიშვნელობის მქონეა.

---

31 უმჯობესია მომწოდებლის მიერ შემოთავაზებულ იქნეს მონაცემთა სტანდარტული ან ღია ფორმატები და ინტერფეისები. ნებისმიერ შემთხვევაში, სახელშეკრულებო პირობები, რომელიც აწესებს სანდო ფორმატებს, ლოგიკური კავშირების შენარჩუნებასა და ნებისმიერ ხარჯს, წარმოშობილს სხვა ღრუბლოვან სისტემაზე მიგრაციით, უნდა იქნეს განხილული.

მეტიც, ღრუბლოვანი სისტემის მომწოდებლებს უნდა გააჩნდეთ შესაბამისი ეფექტური ზომების დოკუმენტალური მტკიცებულებები, რომელიც მიზნად ისახავს წინა პარაგრაფებში აღწერილი მონაცემთა დამუშავების პრინციპების შედეგად მიღებას. მონაცემთა დამუშავების მთელი პროცესის იდენტიფიკაციის უზრუნველყოფა, წვდომის მოთხოვნებზე რეაგირება, რესურების განაწილება, მათ შორის, მონაცემთა დაცვის ოფიცრების დანიშვნა, რომლებიც პასუხისმგებელნი არიან ორგანიზაციის მიერ მონაცემთა დაცვაზე, ან სერტიფიცირების დამოუკიდებელი პროცედურები - წარმოადგენს ამ ზომების მაგალითებს. დამატებით, მონაცემთა დამმუშავებლებმა უნდა უზრუნველყონ მზაობა - მოახდინონ კომპეტენტური ზედამხედველი პირის მიერ, მოთხოვნის შესაბამისად, ზომების დემონსტრირება.[32]

3.5 საერთაშორისო გადაცემები

95/46/EC დირექტივის 25-ე და 26-ე მუხლებით დადგენილია პერსონალურ მონაცემთა თავისუფალი გადაადგილება EEA-ს არაწევრი ქვეყნებისათვის, მხოლოდ იმ შემთხვევაში, თუ მათ გააჩნიათ მონაცემთა დაცვის ადეკვატური დონე. სხვა შემთხვევაში, უნდა იქნეს მიღებული

32 სამუშაო ჯგუფმა შეიმუშავა დეტალური შენიშვნები ანგარიშვალდებულების საკითხის შესახებ თავის მოსაზრებაში 3/2010 ანგარიშვალდებულების პრინციპის შესახებ http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.

დაცვის სპეციალური პირობები დამმუშავებლის და თანადამმუშავებლების ან/და უფლებამოსილი პირების მიერ. თუმცა, ღრუბლოვანი სისტემა უმეტესწილად დაფუძნებულია ღრუბლოვანი სისტემის მომწოდებლის ქსელის მუდმივი მდებარეობის არარსებობაზე. მონაცემი შესაძლებელია ერთ მონაცემთა ცენტრში იყოს დღის ორ საათზე და მსოფლიოს მეორე წერტილში – დღის ოთხ საათზე. ღრუბლოვანი სისტემის მომხმარებელმა იშვიათად იცის, თუ სად იმყოფება, ინახება და გადაიცემა მონაცემები კონკრეტულ დროს. ამ კუთხით, ტრადიციული სამართლებრივი ინსტრუმენტები, რომელიც ადგენს რეგულაციებს მონაცემთა გადაცემის მოწესრიგებისთვის ევროპული კავშირის არაწევრი - მესამე ქვეყნებისთვის, ითვალისწინებს შეზღუდვებს.

3.5.1 Safe Harbor და ადეკვატური დონის მქონე ქვეყნები

ადეკვატურობის დადგენა, მათ შორის Safe Harbor-ის მიხედვით, ლიმიტირებულია გეოგრაფიული არეალის გათვალისწინებით და არ ვრცელდება ღრუბლოვანი სისტემის ფარგლებში არსებულ ყველა გადაცემაზე.

აშშ-ს ორგანიზაციებისთვის პრინციპების დაცვით გადაცემა შესაძლებელია განხორციელდეს ევროპული კავშირის კანონმდებლობის საფუძვე-

ლზე, რამდენადაც მიმღები ორგანიზაციები მიიჩნევიან გადაცემული მონაცემების ადეკვატური დაცვის მქონედ.

თუმცა, სამუშაო ჯგუფის აზრით, Safe Harbor-ის ფარგლებში არსებული მარტოოდენ თვითსერტიფიცირების ფაქტი, შესაძლოა არ იყოს საკმარისი ღრუბლოვან სისტემაში მონაცემთა დაცვის მტკიცე პრინციპების უზრუნველყოფისთვის. ამასთან, დირექტივის მე-17 მუხლი მოითხოვს, რომ ხელშეკრულება გაფორმდეს დამმუშავებლის მიერ უფლებამოსილ პირთან დამუშავების მიზნებიდან გამომდინარე, რომელიც დადასტურებულია ევროპული კავშირი-აშშ Safe Harbor-ის შეთანხმების მასალებთან დაკავშირებულ FAQ 10-ში. აღნიშნული ხელშეკრულება არ ექვემდებარება წინასწარ ავტორიზებას ევროპული კავშირის მონაცემთა დაცვის მარეგულირებელი ორგანოების მიერ. იგი განსაზღვრავს დამუშავების დასაშვებობას და ნებისმიერ ზომას, რომელიც აუცილებელია მონაცემთა უსაფრთხოების უზრუნველსაყოფად. სხვადასხვა ეროვნულ კანონმდებლობას და მონაცემთა დაცვის მარეგულირებელ ორგანოებს შესაძლოა ჰქონდეთ დამატებითი მოთხოვნები.

სამუშაო ჯგუფი მიიჩნევს, რომ კომპანიები, რომლებიც ახდენენ მონაცემთა ექსპორტს არ უნდა დაეყრდნონ მხოლოდ მონაცემთა იმპორ-

ტიორის განცახდებას Safe Harbor-ის ფარგლებში სერთიფიცირების შესახებ. ამის საპირისპიროდ, მონაცემთა ექსპორტიორმა კომპანიამ უნდა მოიპოვოს მტკიცებულება Safe Harbor-ის ფარგლებში თვითსერტიფიცირების შესახებ და მოითხოვოს შესაბამისი პრინციპების დაცვის დამადასტურებელი დოკუმენტი. ეს განსაკუთრებით მნიშვნელოვანია იმ მონაცემთა სუბიექტებისთვის ინფორმაციის მიწოდებისას, რომელთა მონაცემებიც მუშავდება.[33],[34]

სამუშაო ჯგუფი, ასევე, მიიჩნევს, რომ ღრუბლოვანი სისტემის მომხმარებელმა უნდა დაადგინოს არის თუ არა ღრუბლოვანი სისტემის მომწოდებლების სტანდარტული ხელშეკრულებები შედგენილი ისე, რომ თანხვედრაში იყოს მონაცემთა დამუშავებისთვის არსებული ეროვნული კანონმდებლობის სახელშეკრულებო მოთხოვნებთან. ეროვნული კანონმდებლობა შესაძლოა მოითხოვდეს ქვეუფლებამოსილი პირის განსაზღვრას ხელშეკრულებით, რომელიც მოიცავს ქვეკონტრაქტორების ადგილმდებარეობის შესახებ ინფორმაციასა და სხვა მონაცემებს, მათ შორის, მონაცემთა მიკვლევაუნარიანობის პირობას. ჩვეულებრივ, ღრუბლოვანი სისტემის მომწოდებლები

33 იხილეთ გერმანიის მონაცემთა დაცვის ზედამხედველი: http://datenschutz-berlin.de/attachments/710/Resolution_DuesseldorfCircle_28_04_2010EN.pdf.

34 ქვე-კონტრაქტორებთან ხელშეკრულებისთვის არსებული მოთხოვნებისთვის იხილეთ 3.3.2.

არ აწვდიან მომხმარებელს ამგვარ ინფორმაციას – მათ მიერ Safe Harbor პირობების შესრულება ვერ ჩაანაცვლებს აღნიშნული გარანტიების მიღების აუცილებლობას ეროვნული კანონმდებლობის მოთხოვნის შემთხვევაში. ასეთ ვითარებაში, ექსპორტიორს შეუძლია გამოიყენოს სხვა ხელმისაწვდომი სამართლებრივი ინსტრუმენტები, როგორიცაა სტანდარტული სახელშეკრულებო პირობები ან BCR.

და ბოლოს, სამუშაო ჯგუფი მიიჩნევს, რომ Safe Harbor პრინციპებმა ვერ უზრუნველყოფს იმას, რომ მონაცემთა ექსპორტიორმა ღრუბლოვანი სისტემის მწარმოებლს აშშ-ში დაავალოს უსაფრთხოების ისეთი ზომების მიღება, როგორიც მოთხოვნილია ეროვნული კანონმდებლობებით, 95/46/EC დირექტივის საფუძველზე.[35] მონაცემთა უსაფრთხოების კუთხით, ღრუბლოვანი სისტემა ბადებს რამდენიმე მისთვის დამახასიათებელ რისკს უსაფრთხოების კუთხით, როგორიცაა, მართვის დაკარგვა, მონაცემთა დაუცველი ან არასწორი წაშლა, არასაკმარისი შემოწმების გზები ან განცალკევების არარსებობა,[36] რაც არ არის

35 იხილეთ დანიის მონაცემთა დაცვის ზედამხედველის მოსაზრება: http://www.datatilsynet.dk/english/processing-of-sensitive-personal -data-in-a-cloud-solution.

36 დეტალურად აღწერილია ENISA-ს მიერ ღრუბლოვანი სისტემის შესახებ: სარგებელი, რისკები და რეკომენდაციები ინფორმაციული უსაფრთხოებისთვის: https://www.enisa.europa.eu/activities/risk-managment/files/deliverables/cloud-computing-risk-assessment.

საკმარისად განსაზღვრული Safe Harbor-ის პრინციპების მიერ მონაცემთა უსაფრთხოების ჭრილში.[37] დაცვის დამატებითი ზომები შესაძლებელია იქნეს მიღებული მონაცემთა უსაფრთხოებისთვის, როგორიცაა ექსპერტიზა და დამოუკიდებელი პირების ჩართვა, რომლებსაც შეუძლიათ შეაფასონ ღრუბლოვანი სისტემის ადეკვატურობა სხვადასხვა შემოწმების შედეგად, სტანდარტიზაციისა და სერტიფიცირების სქემების გამოყენებით.[38] ამ მიზნით, მიზანშეწონილია მონაცემთა Safe Harbor-ის იმპორტიორის ვალდებულებებს დაემატოს უსაფრთხოების დამატებითი ზომები, რომელიც ითვალისწინებს ღრუბლოვანი სისტემის სპეციფიკურ ბუნებას.

3.5.2 გამონაკლისები

95/46/EC დირექტივის 26-ე მუხლით დადგენილი გამონაკლისები საშუალებას აძლევს მონაცემთა ექსპორტიორებს, დამატებითი გარანტიების არარსებობის შემთხვევაში, გადასცენ მონაცემები ევროპული კავშირის ფარგლებს გარეთ. თუმცა, WP29-მ მიიღო მოსაზრება, სადაც იგი მიიჩნევს, რომ გამონაკლისები გავრცელდება მაშინ, როდესაც მონაცემთა გადაცემა არ არის განმეო-

37 ორგანიზაციებმა უნდა მიიღონ ზომები პერსონალური ინფორმაციის დაკარგვისგან თავის დასაცავად, არამიზნობრივი და არაავტორიზებული წვდომისგან, გამჟღავნებისგან, ცვლილებისა და განადგურებისგან თავიდან ასაცილებლად.
38 იხ. 4.2.

რებადი, მასიური ან სტრუქტურიზებული.[39]

ასეთ შემთხვევაში, ღრუბლოვანი სისტემის კონტექსტში თითქმის შეუძლებელია ამ გამონაკლისებზე დაყრდნობა.

3.5.3 სტანდარტული სახელშეკრულებო პირობები

სტანდარტული სახელშეკრულებო პირობები, რომელიც მიიღო ევროპული კავშირის კომისიამ მონაცემთა საერთაშორისო გადაცემის მოწესრიგებისთვის ორ დამმუშავებელს ან დამმუშავებელსა და უფლებამოსილ პირს შორის, დაფუძნებულია ორმხრივ მიდგომაზე. სადაც ღრუბლოვანი სისტემის მომწოდებელი გვევლინება როგორც უფლებამოსილი პირი. 2010/87/EC მოდალური პირობები წარმოადგენს ინსტრუმენტს, რომელიც შესაძლებელია გამოიყენებოდეს უფლებამოსილ პირსა და დამმუშავებელს შორის, როგორც ღრუბლოვანი სისტემის გარემოში საერთაშორისო ტრანსფერებისთვის ადეკვატური უსაფრთხოების ზომების დამდგენი მექანიზმი.

სტანდარტული სახელშეკრულებო პირობების

39 სამუშაო დოკუმენტი 12/1998: პერსონალურ მონაცემთა გადაცემა მესამე ქვეყნებში: ევროკავშირის მონაცემთა დაცვის დირექტივის 25-ე და 26-ე მუხლების მოქმედება, მიღებული სამუშაო ჯგუფის მიერ 1998 წლის 24 ივლისს. (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf).

გარდა, სამუშაო ჯგუფი აღნიშნავს, რომ ღრუბლოვანი სისტემის მომწოდებლებს შეუძლიათ შესთავაზონ მომხმარებლებს დებულებები, რომელიც დაფუძნებულია მათ პრაგმატულ გამოცდილებაზე იმ მოცულობით, სანამ პირდაპირ ან ირიბად არ შეეწინააღმდეგებიან კომისიის მიერ მიღებულ სტანდარტულ სახელშეკრულებო პირობებს ან მიაყენებს ზიანს მონაცემთა სუბიექტების ძირითად უფლებებსა და თავისუფლებებს.[40] მიუხედავად ამისა, კომპანიებმა არ უნდა ჩაასწორონ ან შეცვალონ სტანდარტული სახელშეკრულებო პირობები დანაწესით, რომ ისინი აღარ იქნება მიჩნეული „სტანდარტულად.“[41]

როდესაც ღრუბლოვანი სისტემის მომწოდებელი დაფუძნებულია ევროპულ კავშირში და მოქმედებს, როგორც უფლებამოსილი პირი, ვითარება შესაძლოა უფრო რთული აღმოჩნდეს, ვინაიდან მოდელური პირობები, ძირითადად, ვრცელდება მხოლოდ ევროპული კავშირის დამმუშავებლისგან არაევროპული კავშირის უფლებამოსილი პირისთვის ტრანსფერზე (იხ. კომისიის გადაწყვე-

40 იხ. ხშირად დასმული კითხვები IV B1.9 9, შეუძლიათ კომპანიებს ჩართონ ხელშეკრულების სტანდარტული პირობები ვრცელ კონტრაქტში და დაამატონ სპეციფიკური პირობები? გამოქვეყნებულია ევროპის კომისიის მიერ
http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf.

41 იხ. ხშირად დასმული შეკითხვები IV B1.10, შეუძლიათ კომპანიებს შეასწორონ ან შეცვალონ ევროპის კომისიის მიერ მიღებული ხელშეკრულების სტანდარტული პირობები?

ტილების პრეამბულა (23) მოდალურ პირობებზე 2010/87/EU და WP176).

რაც შეეხება სახელშეკრულებო ურთიერთობას ევროპული კავშირის უფლებამოსილ პირსა და ქვეკონტრაქტორს შორის, მოდელური პირობებით გათვალისწინებული უნდა იყოს წერილობითი შეთანხმება, რომელიც ადგენს იგივე ვალდებულებებს ქვეკონტრაქტორებისთვის, რაც დადგენილია უფლებამოსილი პირებისთვის.

3.5.4 BCR: გლობალური მიდგომისკენ

BCR წარმოადგენს ქცევის წესების ერთობლიობას იმ კომპანიებისთვის, რომელიც გადასცემენ მონაცემებს თავიანთი ჯგუფის ფარგლებში. ეს მეთოდი იქნება გამოყენებული ღრუბლოვანი სისტემის კონტექსტში, როდესაც მომწოდებელი არის უფლებამოსილი პირი. მართლაც, WP29 ამჟამად მუშაობს BCR-ზე უფლებამოსილი პირებისთვის, რომელიც მონაცემთა გადაცემის საშუალებას მისცემს ჯგუფის ფარგლებში, დამმუშავებლების დავალების შესაბამისად, რითაც თითოეულ მომხმარებელთან დაკავშირებით ხელშეკრულების გაფორმება უფლებამოსილ პირსა და ქვე-დამმუშავებლებს შორის საჭირო აღარ იქნება.[42]

42 იხ. სამუშაო დოკუმენტი 02/2012, რომელიც ადგენს უფლებამოსილი პირის BCR-ში გასაწერი ელემენტებისა და პრინციპების ცხრილს, მიღებული 2012 წლის 6 ივნისს: http://ec.europa.eu/justice/data-protection/

აღნიშნული BCR უფლებამოსილი პირებისთვის, საშუალებას მისცემს მომწოდებლის მომხმარებელს გადაანდოს საკუთარი პერსონალური მონაცემები უფლებამოსილ პირს იმ გარანტიით, რომ გადაცემული მონაცემები მომწოდებლის საქმიანობის ფარგლებში დაცული იქნება უსაფრთხოების ადეკვატური დონით.

4. დასკვნები და რეკომენდაციები

კომპანიები და ადმინისტრაციები, რომლებსაც სურთ გამოიყენონ ღრუბლოვანი სისტემა, პირველ რიგში, უნდა განახორციელონ რისკების სრულყოფილი და ძირეული ანალიზი. აღნიშნული ანალიზი, უნდა აღწერდეს იმ რისკებს, რაც დაკავშირებულია ღრუბლოვან სისტემაში მონაცემთა დამუშავებასთან (კონტროლის ნაკლებობა და არასაკმარისი ინფორმაცია – იხილეთ მე-2 თავი), დამუშავებულ მონაცემთა კატეგორიების გათვალისწინებით.[43] განსაკუთრებული ყურადღება უნდა გამახვილდეს მონაცემთა დამუშავების სამართლებრივ რისკებზე, რომელიც სირთულეს ქმნის, ძირითადად, უსაფრთხოების ვალდებულებებსა და საერთაშორისო გადაცემასთან დაკავშირებით. განსაკუთრებული კატეგორიის პერსონალურ მონაცემთა დამუშავება ღრუბლოვან

article-19/documentation/opinion-recommendation/files/2012/wp195_en.pdf.

43 ENISA განსაზღვრავს იმ რისკების სიას, რომელიც უნდა იქნას მხედველობაში მიღებული http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

სისტემაში წარმოშობს დამატებით სირთულეებს. ასევე, ეროვნული კანონმდებლობის მოთხოვნებისგან დამოუკიდებლად, დამუშავება მოითხოვს დამატებითი უსაფრთხოების პირობებს.[44] წინამდებარე დასკვნები განკუთვნილია იმისათვის, რათა იწარმოოს ე.წ. „ჩეკლისტი“ მონაცემთა დაცვის შესაბამისობისთვის, ღრუბლოვანი სისტემის მომხმარებლებსა და მომწოდებლებს შორის, რომელიც ეფუძნება სამართლებრივ რეგულირებას; ზოგიერთი რეკომენდაცია, ასევე, წარმოდგენილია განვითარების სამომავლო თვალთახედვით ევროპული კავშირის რეგულაციის ფარგლებში და მის მიღმა.

4.1 სახელმძღვანელო დებულებები ღრუბლოვანი სისტემის მომსახურებების მომხმარებლებისა და მომწოდებლებისთვის

- <u>დამმუშავებელი-უფლებამოსილი პირის ურთიერთობა:</u> აღნიშნული მოსაზრება ორიენტირებულია მომხმარებელი-მომწოდებლის, როგორც დამმუშავებელი-უფლებამოსილი პირის ურთიერთობაზე (იხ. პარაგრაფი 3.3.1); თუმცა, კონკრეტულ შემთხვევებში შესაძლებელია წარმოიშვას სიტუაციები, სადაც ღრუბლოვანი სისტემის მომწოდებელი მოქმედებს, როგორც დამმუშავებელი, მაგ. როდესაც მომწოდებელი გადაამუშავებს ზოგიერთ

44 იხ. Sopot მემორანდუმი, მე-2 სქ.

პერსონალურ მონაცემს საკუთარი მიზნებისთვის. ამ შემთხვევაში, ღრუბლოვანი სისტემის მომწოდებელს გააჩნია სრული (თანაზიარი) პასუხისმგებლობა დამუშავების მიმართ და უნდა დააკმაყოფილოს ყველა სამართლებრივი მოთხოვნა, რაც დადგენილია 95/46/EC და 2002/58/EC (გავრცელების შემთხვევაში) დირექტივების მიერ;

- ღრუბლოვანი სისტემის მომხმარებლის, როგორც დამმუშავებლის ვალდებულებები: მომხმარებელი, როგორც დამმუშავებელი, უნდა იყოს პასუხისმგებელი მონაცემთა დაცვის კანონმდებლობის შესრულებაზე. იგი ექვემდებარება ყველა იმ სამართლებრივ მოთხოვნას მონაცემთა სუბიექტების წინაშე, რაც დადგენილია 95/46/EC და 2002/58/EC, გავრცელების შემთხვევაში, დირექტივების მიერ (იხ. 3.3.1). ღრუბლოვანი სისტემის მომხმარებელმა უნდა აირჩიოს ღრუბლოვანი სისტემის ისეთი მომწოდებელი, რომელიც უზრუნველყოფს ევროკავშირის მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობას, რაც გამოიხატება შესაბამისი, ზემოხსენებული სახელშეკრულებო დაცვის მექანიზმების არსებობით;
- უსაფრთხოების ზომები ქვეკონტრაქტირებისას: დებულებები ქვეკონტრაქტირებისთვის უნდა დაინერგოს ღრუბლოვანი სისტემის

მომწოდებელსა და მომხმარებელს შორის დადებულ ნებისმიერ ხელშეკრულებაში, რომელიც უნდა ადგენდეს ქვეკონტრაქტორის პროცესში ჩართვის შესაძლებლობას, მხოლოდ დამმუშავებლის მიერ გაცემული თანხმობის შემთხვევაში და უფლებამოსილი პირის იმ ვალდებულების გათვალისწინებით, რომ აცნობებს დამმუშავებელს ნებისმიერ დაგეგმილ ცვლილებას, ხოლო დამმუშავებელი იტოვებს უფლებას, ნებისმიერ დროს გააპროტესტოს ეს ცვლილებები ან შეწყვიტოს ხელშეკრულება. ღრუბლოვანი სისტემის მომწოდებელს უნდა ჰქონდეს აშკარა ვალდებულება დაასახელოს დამუშავებაში მონაწილე ყველა ქვეკონტრაქტორი. მანვე უნდა გააფორმოს კონტრაქტი თითოეულ ქვეკონტრაქტორთან, რომელიც შესაბამისობაშია ღრუბლოვანი სისტემის მომხმარებელთან გაფორმებული ხელშეკრულების პირობებთან; მომხმარებელმა უნდა უზრუნველყოს, მომწოდებლის ქვეკონტრაქტორთა მიერ სახელშეკრულებო ვალდებულების დარღვევის შემთხვევაში ხელშეკრულებით გათვალისწინებული რეაგირების საშუალებების არსებობა (იხ. 3.3.2).

- <u>მონაცემთა დაცვის ძირითად პრინციპებთან შესაბამისობა:</u>

– გამჭვირვალობა (იხ. 3.4.1.1): სახელშეკრულებო პირობებზე მოლაპარაკებებისას ღრუ-

ბლოვანი სისტემის მწარმოებლებმა უნდა მოახდინონ ღრუბლოვანი სისტემის მომხმარებლის ინფორმირება მომსახურების ყველა (მონაცემთა დაცვის) რელევანტური ასპექტის შესახებ; კერძოდ, მომხმარებლები უნდა იყვნენ ინფორმირებულნი ყველა ქვეკონტრაქტორის შესახებ, რომელიც ფუნქციონირებს ხსენებული ღრუბლოვანი სისტემის მომსახურებისას და ინფორმირებული ყველა იმ ადგილის შესახებ, სადაც შესაძლებელია მონაცემი შენახულ იქნეს ან დამუშავდეს ღრუბლოვანი სისტემის მომწოდებლის ან/და მათი ქვეკონტრაქტორების მიერ (განსაკუთრებით მაშინ, თუ რომელიმე ან ყველა ადგილმდებარეობა არის EEA-ს ფარგლებს გარეთ); მომხმარებელი უნდა იყოს ინფორმირებული მომწოდებლის მხრიდან დანერგილი ტექნიკური და ორგანიზაციული ზომების შესახებ; საუკეთესო მაგალითის თანახმად, მომხმარებელმა უნდა მოახდინოს მონაცემთა სუბიექტების ინფორმირება ღრუბლოვანი სისტემის მომწოდებლისა და ქვეკონტრაქტორების შესახებ (არსებობის შემთხვევაში), ასევე, იმ ადგილმდებარეობის შესახებ სადაც მონაცემი შესაძლებელია იქნეს შენახული ან დამუშავდეს ღრუბლოვანი სისტემის მომწოდებლის ან/და ქვეკონტრაქტორის მიერ;

– მიზნის კონკრეტულობა და ლიმიტირება

(3.4.1.2): მომხმარებელმა უნდა უზრუნველყოს შესაბამისობა მიზნის კონკრეტულობისა და ლიმიტირების პრინციპებთან და უზრუნველყოს, რომ მომწოდებლის ან რომელიმე ქვეკონტრაქტორის მხრიდან მონაცემთა სხვა მიზნებისთვის დამუშავებას არ ექნება ადგილი. ვალდებულებები ამ კუთხით, უნდა გამყარდეს შესაბამისი სახელშერკრულებო ზომებით (მათ შორის, ტექნიკური და ორგანიზაციული უსაფრთხოების პირობებით).

– მონაცემთა შენახვა (3.4.1.3): ღრუბლოვანი სისტემის მომხმარებელი პასუხისმგებელია პერსონალურ მონაცემთა შენახვის ადგილიდან წაშლაზე (მომწოდებლის ან ქვეკონტრაქტორების მიერ), მაშინვე როდესაც იგი აღარ არის საჭირო შესაბამისი მიზნისთვის; წაშლის უსაფრთხო მექანიზმები (განადგურება, დემაგნეტიზირება, გადაწერა) უნდა იყოს განმტკიცებული ხელშეკრულებით;
– <u>უსაფრთხოების სახელშეკრულებო პირობები (იხ. 3.4.2, 3.4.3 და 3.5):</u>
– ძირითადად, მწარმოებელთან დადებული ხელშეკრულება (ასევე ის ხელშეკრულებები, რომლებიც გაფორმებულია მომწოდებელსა და ქვეკონტრაქტორებს შორის) ტექნიკური უსაფრთხოებისა და ორგანიზაციული ზომების საკმარის გარანტიებს უნდა უზრუნველყოფდეს (დირექტივის მე-17(2) მუხლის შესა-

ბამისად) და უნდა იყოს ფორმულირებული წერილობით ან სხვა ექვივალენტური ფორმით. ხელშეკრულება უნდა ადგენდეს მომხმარებლის დეტალურ ინსტრუქციებს მომწოდებლის მიმართ, რომელიც მოიცავს მომსახურების საგანსა და ვადებს, მომსახურების მიზნობრივ და გაზომვად ხარისხს და სათანადო სანქციებს (ფინანსურ ან სხვაგვარს); იგი უნდა ადგენდეს უსაფრთხოების ზომებს, რომელიც უნდა იყოს დამუშავების რისკებისა და მონაცემთა ბუნების ადეკვატური, ზემოხსენებული ვალდებულებების გათვალისწინებით და მეტად მკაცრი ზომების თანხლებით, რაც დადგენილია მომხმარებლის შიდასახელმწიფოებრივი კანონმდებლობით; თუ ღრუბლოვანი სისტემის მწარმოებლებს სურთ გამოიყენონ სტანდარტული სახელშეკრულებო პირობები, მათ უნდა უზრუნველყონ ამ პირობების შესაბამისობა მონაცემთა დაცვის მოთხოვნებთან (იხ. 3.4.2); კერძოდ, ის ტექნიკური და ორგანიზაციული ზომები, რაც დაინერგა მომწოდებლის მიერ უნდა აისახოს შესაბამისი ჩანაწერით;

– მონაცემებთან წვდომა: მხოლოდ ავტორიზებულ პირებს უნდა ჰქონდეთ წვდომა მონაცემებთან; მომწოდებლისა და მისი დასაქმებულების ხელშეკრულებაში უნდა განისაზღვროს კონფიდენციალურობის პირობა;

– მესამე პირებისთვის მონაცემთა გამჟღავნება: აღნიშნული უნდა იყოს დარეგულირებული მხოლოდ ხელშეკრულებით, რომელიც უნდა მოიცავდეს მომწოდებლის ვალდებულებას, დაასახელოს ყველა მისი ქვეკონტრაქტორი – მაგ. საჯარო ციფრული რეესტრი – და უზრუნველყოს მომხმარებლისთვის ინფორმაციის მიწოდება ნებისმიერი ცვლილებისას, იმ მიზნით, რომ მომხმარებელს უფლება ჰქონდეს გააპროტესტოს ცვლილება ან შეწყვიტოს ხელშეკრულება; ხელშეკრულებით მომწოდებელი უნდა იყოს ვალდებული, პერსონალურ მონაცემთა გამჟღავნების შემთხვევაში, აცნობოს თოთოეული იმ სამართლებრივად სავალდებულო მოთხოვნების შესრულების შესახებ, რომელიც განსაზღვრულია სამართალდამცავი ორგანოს მიერ, თუ ამგვარი გამჟღავნება სხვა შემთხვევაში აკრძალულია; ღრუბლოვანი სისტემის მომხმარებელმა უნდა უზრუნველყოს, რომ მომწოდებელი არ შეასრულებს რომელიმე სამართლებრივად არასავალდებულო მოთხოვნას გამჟღავნების შესახებ;
– თანამშრომლობის ვალდებულებები: მომხმარებელმა უნდა უზრუნველყოს, მომწოდებლის თანამშრომლობა მომხმარებელთან, რათა განახორციელოს დამუშავების პროცესის მონიტორინგი და ხელი შეუწყოს მონა-

ცემთა სუბიექტების მონაცემების წვდომის/შესწორების/წაშლის უფლებების რეალიზაციას, ასევე (სადაც სავალდებულოა) აცნობოს ღრუბლოვანი სისტემის მომხმარებელს მონაცემთა ნებისმიერი დარღვევის შესახებ, რომელიც გავლენას ახდენს მომხმარებლის მონაცემებზე;

– მონაცემთა ტრანსსასაზღვრო გადაცემა: ღრუბლოვანი სისტემის მომხმარებელი უნდა დარწმუნდეს, შეუძლია თუ არა მომწოდებელს მონაცემთა ტრანსსასაზღვრო გადაცემისას კანონიერების გარანტირება და ტრანსფერების ლიმიტირება მომხმარებლის მიერ არჩეული ქვეყნების შესაბამისად, შესაძლებლობის შემთხვევაში. მონაცემთა ტრანსფერი ადეკვატური დონის არმქონე ქვეყნებში მოითხოვს შესაბამისი უსაფრთხოების დონის განმტკიცებას Safe Harbor-ის დებულებების, სტანდარტული სახელშეკრულებო პირობების (SCC) ან BCR-ს მეშვეობით; სტანდარტული სახელშეკრულებო პირობების გამოყენება უფლებამოსილი პირებსთვის (კომისიის 2010/87/EC გადაწყვეტილების შესაბამისად) მოითხოვს სათანადო მორგებას ღრუბლოვანი სისტემის გარემოზე (რათა თავიდან ავიცილოთ ხელშეკრულებების ცალკეულად გაფორმება თითოეული მომხმარებლის გათვალისწინებით მომწოდებელსა და ქვე-

კონტრაქტორს შორის), რომელიც შესაძლოა ადგენდეს მონაცემთა დაცვის მარეგულირებელი უფლებამოსილი ორგანოს წინასწარ ავტორიზებას; ხელშეკრულებაში უნდა აისახოს იმ ადგილმდებარეობების სია, სადაც მომსახურება შეიძლება განხორციელდეს;

– დამუშავების ოპერაციათა შენახვა და შემოწმება: მომხმარებელმა უნდა მოითხოვოს მომწოდებლისა და ქვეკონტრაქტორების მხრიდან წარმოებული დამუშავების ოპერაციათა შენახვა; მომხმარებელს უნდა ჰქონდეს უფლებამოსილება შეამოწმოს ამგვარი დამუშავების პროცესი, თუმცა, მაქსიმალური გამჭვირვალობის უზრუნველსაყოფად, ასევე, შესაძლებელია მიზანშეწონილი იყოს დამმუშავებლის მიერ არჩეული დამოუკიდებელი აუდიტი და სერტიფიცირება (მაგ. იმის შესაძლებლობა, რომ გაიცეს დამოუკიდებელი აუდიტის სერტიფიკატის ასლი ან აუდიტის დასკვნის ასლი, რითაც დგინდება სერტიფიცირება).

– ტექნიკური და ორგანიზაციული ზომები: იგი უნდა ისახავდეს მიზნად იმ რისკების შემცირებას, რაც გამოწვეულია კონტროლისა და ინფორმაციის ნაკლებობით და დამახასიათებელია ღრუბლოვანი სისტემის გარემოსთვის. ეს უკანასკნელი მოიცავს ზომებს, რომელიც მიმართულია ხელმისაწვდომობის, ნამდვი-

ლობის, კონფიდენციალურობის, განცალკევების, ჩარევაუნარიანობის, პორტატულობისა და გამჭვირვალობის მიღწევისთვის, ისეთი სახით, როგორც აღნიშნულია ამ დოკუმენტში (დეტალურად, იხ. 3.4.3).

4.2 მონაცემთა დაცვის სერტიფიცირება დამოუკიდებელი პირების მიერ

- კარგი რეპუტაციის მქონე დამოუკიდებელი პირის მიერ ღრუბლოვანი სისტემის მომწოდებლის სერტიფიცირება ან დამოწმება შესაძლოა იყოს ეფექტური საშუალება, რათა მოხდეს აღნიშნულ მოსაზრებაში წარმოდგენილ ვალდებულებებთან შესაბამისობის დემონსტრირება. ამგვარი სერტიფიცირება უნდა ავლენდეს, რომ შემოწმდა ან გადაიხედა მონაცემთა დაცვის მართვა დამოუკიდებელი, მაღალი რეპუტაციის მქონე ორგანიზაციის მიერ, აღიარებული სტანდარტის შესაბამისად, რომელიც თანხვედრაშია ამ მოსაზრებით განმტკიცებულ მოთხოვნებთან.[45] ღრუბლოვანი სისტემის კონტექსტში, პოტენციური მომხმარებლები უნდა დაინტერესდ-

45 ასეთი სტადარტები მოიცავს მათ, რომელიც გამოცემულია სტანდარტების საეთაშორისო ორგანიზაციის, საერთაშორისო აუდიტისა და გარანტირების სტანდარტული ბორდისა და ამერიკის სერტიფიცირებული საჯარო ბუღალტრების აუდიტის სტანდარტული ბორდის მიერ, რამდენადაც ეს ორგანიზაციები ადგენენ სტანდარტებს, რომელიც უნდა იქნას დაკმაყოფილებული ამ მოსაზრების თანახმად.

ნენ, თუ რამდენად შეუძლიათ ღრუბლოვანი სისტემის მწარმოებლებს დამოუკიდებელი პირის მიერ ჩატარებული შემოწმების სერტიფიკატის ან შემოწმების დასკვნის ასლის წარმოდგენა, რითაც დგინდება სერტიფიცირება მოსაზრებაში მოცემული მოთხოვნების გათვალისწინებით.

- სხვადასხვა ადგილას და ვირტუალური სერვერის გარემოში განთავსებული მონაცემების ინდივიდუალური შემოწმება, შესაძლოა ტექნიკურად შეუძლებელი აღმოჩნდეს და ამავე დროს, საფრთხე შეექმნას ქსელის ლოგიკური და ფიზიკური უსაფრთხოების მართვას. ამ შემთხვევაში, დამმუშავებლის მიერ არჩეული დამოუკიდებელი შემოწმება, ცალკეული დამმუშავებლისთვის შესაძლოა ჩაითვალოს დამაკამყოფილებლად შემოწმების უფლების უზრუნველყოფის მხრივ.
- პრივატულობაზე მორგებული სტანდარტების მიღება და სერტიფიცირება წარმოადგენს ცენტრალურ საკითხს ღრუბლოვანი სისტემის მწარმოებლებს, დამმუშავებლებსა და მონაცემთა სუბიექტებს შორის, სანდო ურთიერთობის დასამყარებლად.
- ეს სტანდარტები და სერტიფიცირებები უნდა მოიცავდეს ტექნიკურ ზომებს (როგორიცაა მონაცემთა კრიპტაციის ლოკალიზება), ასევე პროცესებს ღრუბლოვანი სისტემის მომწოდებლის ორგანიზაციის ფარგლებში, რაც

უზრუნველყოფს მონაცემთა დაცვას (როგორიცაა წვდომის კონტროლის პოლიტიკა, წვდომის კონტროლი ან რეზერვაცია).

4.3 რეკომენდაციები: სამომავლო განვითარება

სამუშაო ჯგუფი აცნობიერებს, რომ ღრუბლოვანი სისტემის კომპლექსური თავისებურებები სრულად ვერ იქნება გარანტირებული მოსაზრებაში განხილული უსაფრთხოების ზომებისა და გადაწყვეტების მეშვეობით, მიუხედავად იმისა, რომ ის ადგენს მძლავრ საფუძველს პერსონალურ მონაცემთა დამუშავების უსაფრთხოებისთვის EEA-ს მომხმარებლების ღრუბლოვანი სისტემის მომწოდებლებისთვის. ეს ნაწილი მიმართულია იმისკენ, რომ ხაზი გაუსვას ზოგიერთ საკითხს, რომელიც უნდა გადაწყდეს დროის მოკლე პერიოდში უსაფრთხოების ზომების გაზრდისა და ღრუბლოვანი სისტემის მხარდაჭერისთვის ამ საკითხების ჭრილში, მონაცემთა დაცვისა და პრივატულობის ფუნდამენტური უფლებების დაცვის უზრუნველსაყოფად.

- დამმუშავებელსა და უფლებამოსილ პირს შორის პასუხისმგებლობათა უკეთესი დაბალანსება: სამუშაო ჯგუფი მიესალმება კომისიის კანონპროექტის (ევროკავშირის მონაცემთა დაცვის ძირითადი რეგულაციის შესახებ) 26-ე მუხლის დანაწესს, რომელიც მიმართულია უსაფრთხოებასთან დაკავშირებული

პირობების განმტკიცებისკენ, უფლებამოსილი პირების მეტი ანგარიშვალდებულებით დამმუშავებლების მიმართ. კანონპროექტის 30-ე მუხლი ადგენს სამართლებრივ ვალდებულებას უფლებამოსილი პირისათვის, რომ მოახდინოს შესაბამისი ტექნიკური და ორგანიზაციული ზომების იმპლემენტაცია. კანონპროექტი განმარტავს, რომ უფლებამოსილი პირი, რომელიც ვერ ასრულებს დამმუშავებლის ინსტრუქციებს მიიჩნევა მონაცემთა დამმუშავებლად და ექვემდებარება თანადამუშავების სპეციფიკურ წესებს. WP29 აცნობიერებს, რომ ეს კანონპროექტი სწორი მიმართულებით არის ფორმულირებული, რათა აღმოფხვრას ღრუბლოვანი სისტემის გარემოსთვის დამახასიათებელი დისბალანსი, სადაც მომხმარებლისთვის (განსაკუთრებით თუ იგი არის მცირე ან საშუალო ორგანიზაცია) რთულია განხორციელდეს მონაცემთა დაცვის კანონმდებლობით მოთხოვნილი სრული კონტროლი მომწოდებელის მიერ მოთხოვნილი მომსახურების მიწოდებაზე. მეტიც, მონაცემთა სუბიექტებისა და მცირე ბიზნესის მომხმარებლების ასიმეტრიული სამართლებრივი პოზიციიდან გამომდინარე (უფლებრივად) დიდი ღრუბლოვანი სისტემის მწარმოებლებთან მიმართებით, ორგანიზაციების მომხმარებლისა და ბიზნეს ინტერესე-

ბის გათვალისწინებით, რეკომენდირებულია მეტად პროაქტიული მოქმედება, რათა კომპანიებისთვის მაქსიმალურად დაბალანსებული ძირითადი პირობები განისაზღვროს.

- პერსონალურ მონაცემებთან წვდომა ეროვნული უსაფრთხოებისა და სამართალდაცვითი მიზნებისთვის: უაღრესად მნიშვნელოვანია სამომავლო რეგულაციას დაემატოს დამმუშავებლების მიერ მესამე ქვეყნებისთვის პერსონალურ მონაცემთა გამჟღავნების აკრძალვა, თუ აღნიშნული მოთხოვნილია მესამე ქვეყნის მართლმსაჯულების ან აღმასრულებელი ორგანოების მიერ, გარდა იმ შემთხვევებისა, თუკი აღნიშნული აშკარად ნებადართულია საერთაშორისო ხელშეკრულებით, სამართლებრივი ურთიერთდახმარების შესახებ შეთანხმებით ან ზედამხედველი ორგანოს მიერ. საბჭოს რეგულაცია (EC) 2271/96 ზემოაღნიშნულისთვის წარმოადგენს შესაბამის სამართლებრივ საფუძველს.[46] სამუშაო ჯგუფი შეშფოთებულია კომისიის კანონპროექტის ამ ხარვეზით, რამდენაც სახეზეა სამართლებრივი სიზუსტის საგრძ-

46 1996 წლის 22 ნოემბრის საბჭოს რეგულაცია (EC) 2271/96 მესამე ქვეყნების კანონმდებლობის ექსტრა-ტერიტორიალური გავლენისგან დაცვის შესახებ, იმ ქმედებებისა და შედეგებისგან დაცვის შესახებ რომელიც გამომდინარეობს ზემოაღნიშნულიდან, ოფიციალური გამომცემლობა L 309, 29/11/1996 P. 0001 – 0006, ვებ-გვერდი:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996R2271:EN:HTML.

ნობი ნაკლებობა იმ მონაცემთა სუბიექტებისთვის, რომელთა პერსონალური მონაცემები ინახება მონაცემთა ცენტრებში მთელი მსოფლიოს მასშტაბით. ამ მიზეზით, სამუშაო ჯგუფს სურს რეგულაციაში ხაზი გაესვას[47] ურთიერთშეთანხმების ხელშეკრულებების შესახებ დებულებების სავალდებულო გამოყენებას, იმ შემთხვევაში თუკი გამჟღავნდება მონაცემები კავშირის ან წევრი ქვეყნების კანონმდებლობის საფუძველზე ავტორიზების არ არსებობის შემთხვევაში.

- განსაკუთრებული სიფრთხილე საჯარო სექტორში: განსაკუთრებული სიფრთხილე უნდა გამოვლინდეს საჯარო სექტორის მხრიდან, რათა შეფასდეს წარმოშობს თუ არა რისკებს ეროვნული ტერიტორიის ფარგლებს გარეთ მონაცემთა კომუნიკაცია, დამუშავება და შენახვა მოქალაქეთა უსაფრთხოების, პრივატულობის, ეროვნული და ეკონომიკური უსაფრთხოების კუთხით, კერძოდ, თუკი პროცესში ჩართულია განსაკუთრებული კატეგორიის მონაცემთა ბაზები (მაგ. დემოგრაფიული მონაცემები) და მომსახურებები (მაგ. ჯანმრთელობის დაცვა).[48] ამ მხრივ, გან-

47 იხ. WP191 – მოსაზრება 01/2012 მონაცემთა დაცვის რეფორმის კანონპროექტის შესახებ, გვ. 23.

48 ამ მხრივ, ENISA ადგენს წინამდებარე რეკომენდაციას მის დოკუმენტში უსაფრთხოებისა და მოქნილობის შესახებ სამთავრობო ღრუბლოვან სისტემაში (http://www.enisa.europa.eu/activities/risk-managment/emerging-and-future-risk/deliverables/security-and-re-

საკუთრებული ყურადღება უნდა დაეთმოს ნებისმიერ შემთხვევას, როდესაც განსაკუთრებული კატეგორიის მონაცემები მუშავდება ღრუბლოვან სისტემაში. ამ თვალსაზრისით, ყურადღება შესაძლოა გამახვილდეს შიდასახელმწიფოებრივი მთავრობების და ევროპული კავშირის ინსტიტუტებზე, რათა სამომავლოდ გამოკვლეულ იქნეს ევროპული სამთავრობო ღრუბლოვანი სისტემის, როგორც სახელმწიფოთაშორისი ვირტუალური გარემოს, კონცეფცია, სადაც გამოყენებული იქნება ნორმათა შეთანხმებული და ჰარმონიზებული ერთობლიობა.

- ევროპული ღრუბლოვანი სისტემის კოოპერაცია: სამუშაო ჯგუფი მხარს უჭერს ევროპული ღრუბლოვანი სისტემის კოოპერაციის სტრატეგიას, რომელიც წარმოადგინა ევროპული კომისიის ვიცეპრეზიდენტმა, ქ-ნმა კროესმა, 2012 წლის იანვარში, დავოსში.[49] სტრატეგია

---

silience-in-governmental-clouds/at_download/fullReport):

„არქიტექტურის გათვალისწინებით, სენსიტიური აპლიკაციებისთვის, დახურული და გაერთიანების ღრუბლოვანი სისტემები წარმოგვიდგება ისეთად, რომელიც ყველაზე მეტად ერგება საჯარო ადმინისტრაციების საჭიროებებს, რამდენადაც ისინი ახორციელებენ მმართველობის, კონტროლისა და გამჭვირვალობის უმაღლეს დონეს, და მიუხედავად იმისა, რომ ხდება დახურული ან გაერთიანების ღრუბლოვანი სისტემის დანერგვა, განსაკუთრებული ყურადღება უნდა გამახვილდეს ინფრასტრუქტურის მოწყობაზე.“

49 ნელი კროესი, ევროპული კომისიის ვიცე პრეზიდენტი, პასუხისმგებელი ციფრულ გეგმაზე, ევროპული ღრუბლოვანი სისტემის თანამშრომლობის ჩამოყალიბება, მსოფლიო ეკო-

მოიცავს საჯარო IT უზრუნველყოფას, რომელიც აბალანსებს ევროპული ღრუბლოვანი სისტემის ბაზარს. დამოუკიდებლად მართული მონაცემთა დაცვის ევროპული კანონმდებლობის გამოყენებით ევროპული ღრუბლოვანი სისტემის მომწოდებლის მიერ პერსონალურ მონაცემთა გადაცემა, შესაძლებელია გახდეს დიდი სარგებლის მომტანი მომხმარებლებისთვის, როგორც მონაცემთა დაცვის მხრივ, კერძოდ, საერთო სტანდარტების მიღების ხელშეწყობიდან გამომდინარე (განსაკუთრებით, ჩარევაუნარიანობისა და მონაცემთა პორტატულობის მხრივ), ისე სამართლებრივი სიზუსტის მხრივ.

ნომოკური ფორუმი, დავოსი, შვეიცარია, 2012 წლის 26 იანვარი, ვებ-გვერდი: http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/1_23.

დანართი

ა) წარმოების მოდელები

დახურული ღრუბლოვანი სისტემა[50] გულისხმობს IT ინფრასტრუქტურას, რომელიც განკუთვნილია კონკრეტული ორგანიზაციისთვის; იგი მდებარეობს ორგანიზაციის შენობაში ან მისი მართვა აუთსორსირებულია მესამე მხარისათვის (ძირითადად, სერვერის ჰოსტინგით), რომელიც იმყოფება დამმუშავებლის მკაცრი ზედამხედველობის ქვეშ. დახურული ღრუბლოვანი სისტემა შესაძლებელია შევადაროთ ჩვეულებრივ მონაცემთა ცენტრს – იმ განსხვავებით, რომ ტექნოლოგიური

50 NIST (სტანდარტებისა და ტექნოლოგიის ეროვნული ინსტიტუტი) აშშ-ში, რომელიც რამოდენიმე წელი მუშაობდა ღრუბლოვან სისტემაზე დაფუძნებული ტექნოლოგიების[50] სტანდარტიზაციაზე და რომლის განმარტებები ასევე მითითებულია ENISA-ს დოკუმენტში:

დახურული ღრუბლოვანი სისტემა.

ღრუბლოვანი სისტემის ინფრასტრუქტურა ფუნქციონირებს მხოლოდ ორგანიზაციისთვის. იგი შეიძლება იყოს მართული ორგანიზაციის ან მესამე პირის მიერ და არსებობდეს დაწესებულებაში ან მის გარეთ. უნდა აღინიშნოს, რომ „დახურული ღრუბლოვანი სისტემა“ ეფუძნება კონკრეტულ ტექნოლოგიებს, რომელიც ასევე დამახასიათებელია „საჯარო ღრუბლოვანი სისტემებისთვის“- მათ შორის, ტექნოლოგიების ვირტუალიზაცია, რაც ხელს უწყობს მონაცემთა დამუშავების არქიტექტურის რეორგანიზაციას (ან შეკეთებას), როგორც ზემოთ იქნა აღნიშნული.

საჯარო ღრუბლოვანი სისტემა.

ღრუბლოვანი სისტემის ინფრასტრუქტურა არის ხელმისაწვდომი საჯაროდ ან მსხვილი ინდუსტრიული ჯგუფის შიგნით და ეკუთვნის ორგანიზაციას, რომელიც ჰყიდის ღრუბლოვანი სისტემის მომსახურებებს.

გადაწყვეტები იმპლემენტირებულია ხელმისაწვდომი რესურსების ოპტიმალურად გამოყენებისთვის და ამ რესურსების მცირე ინვესტიციების მეშვეობით გაძლიერებით, რაც ხორციელდება ეტაპობრივად დროთა განმავლობაში.

აღნიშნულის საპირისპიროდ, საჯარო ღრუბლოვანი სისტემა წარმოადგენს ინფრასტრუქტურას, რომელიც მომწოდებლის მფლობელობაშია და მიმართულია მომსახურებების მიწოდებაზე – შესაბამისად გაზიარებაზე – მისი სისტემების მომხმარებლებისთვის ან, მათ შორის, საწარმოებსა და სახელმიწიფო ორგანოებისთვის. ამ მომსახურების მიღება შესაძლებელია ინტერნეტის გამოყენებით, რომელიც მოიცავს მონაცემთა დამუშავების ოპერაციათა ან/და მონაცემების ტრანსფერს მომსახურების მომწოდებლისთვის. გამომდინარე აქედან, მომსახურების მომწოდებელი თამაშობს გადამწყვეტ როლს იმ მონაცემთა ეფექტური დაცვისთვის, რაც გადაეცა მის სისტემას. მონაცემებთან ერთად, მომხმარებელი ვალდებულია მოახდინოს საკუთარი კონტროლის შესაძლებლობის საგრძნობი გავრცელება ამ მონაცემებზე.

საჯარო და დახურულ ღრუბლოვან სისტემებთან ერთად, არსებობს ე.წ. „შერეული“ ან „ჰიბრიდული“ ღრუბლოვანი სისტემები, სადაც დახურული ინფრასტრუქტურების მიერ წარმოებული მომ-

სახურებები საჯარო ღრუბლოვანი სისტემებიდან შეძენილ მომსახურებებთან ერთად ფუნქციონირებს. აღსანიშნავია, ასევე, „გაერთიანების ღრუბლოვანი სისტემები," სადაც გაერთიანების მომხმარებლებისთვის IT ინფრასტრუქტურა გაზიარებულია რამოდენიმე ორგანიზაციის მიერ.

ღრუბლოვანი სისტემების კონფიგურირების მოქნილობა და სიმარტივე უზრუნველყოფს მათ მოქნილობას, ანუ ეს სისტემები შესაძლებელია მოერგოს კონკრეტულ მოთხოვნებს, რომელიც შესაბამისობაშია მისი გამოყენების თავსებურებებთან. მომხმარებლებს არ უწევთ აუთსორსის შეთანხმებებზე დაფუძნებული რომელიმე IT სისტემის მართვა, რაც, შესაბამისად, იმართება მთლიანად მესამე პირის მიერ, რომლის ღრუბლოვან სისტემაშიც არის მონაცემები შენახული. ხშირია შემთხვევები, როდესაც დიდი მასშტაბის მომწოდებლები მოქმედებენ კომპლექსური ინფრასტრუქტურით; ამიტომ, ღრუბლოვანი სისტემა შესაძლებელია მოიცავდეს რამოდენიმე ადგილმდებარეობას ერთდროულად და მომხმარებლებმა კი, ყურადღება არ მიაქციონ იმას, თუ ზუსტად სად ინახება მათი მონაცემი.

ბ) მომსახურების მიწოდების მოდელები

მომხმარებლის მოთხოვნილებიდან გამომდინარე, არსებობს ბაზარზე ხელმისაწვდომი ღრუბლო-

ვანი სისტემის რამოდენიმე მოდელი; ისინი შესაძლოა დაჯგუფებულ იქნას 3 ძირითად კატეგორიად ან მომსახურების მოდელად. ეს მოდელები ძირითადად გამოიყენება, როგორც დახურული, ისე საჯარო ღრუბლოვანი სისტემის ფუნქციონირებისას:

- IaaS (Cloud Infrastructure as a Service - ღრუბლოვანი ინფრასტრუქტურა, როგორც მომსახურება): მომწოდებელი აქირავებს ტექნოლოგიურ ინფრასტრუქტურას, ანუ დისტანციურ ვირტუალურ სერვერებს იმგვარად, რომ მის საბოლოო მომხმარებელს შეუძლია გამოიყენოს იგი იმ მექანიზმებითა და გადაწყვეტებით, რომელიც კომპანიის შენობაში კორპორატიული IT სისტემის ჩანაცვლებას მარტივს, ეფექტურს და სასარგებლოს გახდის ან/და გამოიყენებს დაქირავებულ ინფრასტრუქტურას კორპორატიულ სისტემებთან ერთად. აღნიშნულ მწარმოებლებს ძირითადად წარმოადგენენ ბაზრის სპეციალიზებული მონაწილეები, რომლებიც მოქმედებენ რამოდენიმე გეოგრაფიულ არეალში მდებარე ფიზიკურ, კომპლექსურ ინფრასტრუქტურაზე.
- SaaS (Cloud Software as a Service - ღრუბლოვანი პროგრამული უზრუნველყოფა, როგორც მომსახურება): მომწოდებელი ვების გამოყენებით აწვდის სხვადასხვა პროგრამულ მომსახურებას და ხდის მათ ხელმისაწვდომს

საბოლოო მომხმარებლისთვის. ძირითადად, აღნიშნული მომსახურებები გამოიყენება ჩვეულებრივი პროგრამების ჩასანაცვლებლად, რომელიც დაყენებულია მომხმარებლების მიერ საკუთარ ადგილობრივ სისტემებზე; შესაბამისად, მომხმარებლები ახდნენ მათი მონაცემების აუთსორსს კონკრეტულ მწარმოებელზე. ეს ხდება, ტიპური ვებზე დაფუძნებული საოფისე პროგრამების, როგორიცაა ცხრილების, ტექსტის რედაქტირების საშუალებების, კომპიუტერული რეესტრების, დამგეგმავების, საზიარო კალენდრებისა და ა.შ. გამოყენებისას; ამასთან, აღნიშნული მომსახურებები მოიცავს ღრუბლოვან სისტემაზე დაფუძნებულ ელ-ფოსტის პროგრამებსაც.

- PaaS (Cloud Platform as a Service, ღრუბლოვანი პლატფორმა, როგორც მომსახურება): მომწოდებელი სთავაზობს მეთოდებს აპლიკაციების მოწინავე განვითარებისა და ჰოსტინგისთვის. ეს მომსახურებები, ძირითადად, მიმართულია ბაზრის იმ მონაწილეებისთვის, რომლებიც იყენებენ მას, დასაკუთრების ფუნქციის სახის პროგრამული გადაწყვეტების შესაქმენლად და მისი ჰოსტინგისათვის, შიდა მოთხოვნების დასაკმაყოფილდებლად ან/და მესამე პირებისთვის მომსახურების საწარმოებლად. ისევ და ისევ, მომსახურებები რო-

მელიც მოწოდებულია PaaS მომწოდებლის მიერ, მომხმარებლის მხრიდან დამატებითი ან/და სპეციალური მოწყობილობის გამოყენებას ან პროგრამულ უზრუნველყოფას შიდა დონეზე უსარგებლოს ხდის.

საჯარო ღრუბლოვანი სისტემების სრული ჩართვა მოკლე ვადების გათვალისწინებით ვერ იქნება შესაძლებელი რამოდენიმე მიზეზის გამო, რაც ძირითადად ეხება დიდი კომპანიებს ან ორგანიზაციებს, რომლებმაც უნდა დააკმაყოფილონ სპეციალური ვალდებულებები – მაგ. ბანკები, სამთავრობო ორგანოები, დიდი მუნიციპალიტეტები და ა.შ. ეს შეიძლება გამოწვეული იყოს ორი ძირითადი მიზეზით: ამგვარ გადაცემასთან დაკავშირებით მოთხოვნილ ინვესტიციებთან; მეორე, მხედველობაში უნდა მივიღოთ განსაკუთრებით ღირებული ან/და განსაკუთარებული კატეგორიის ინფორმაცია, რომელიც კონკრეტულ სიტუაციებში უნდა დამუშავდეს.

კიდევ ერთი ფაქტორი, რაც ამტკიცებს დახურული ღრუბლოვანი სისტემის გამოყენების უპირატესობას (ზემოხსენებულ შემთხვევებში მაინც) არის ის, რომ საჯარო ღრუბლოვანი სისტემის მომწოდებელს, ხშირ შემთხვევაში, არ შეუძლია უზრუნველყოს მომსახურების ხარისხი (როგორც განსაზღრვულია SLA (Service Level Agreement)

შეთანხმებით), რათა შესაბამისობაში იყოს დამმუშავებლისთვის მიწოდებულ მომსახურებების ბუნებასთან. ეს ალბათ იმიტომ, რომ კონკრეტული მომხმარებელი-მომწოდებლის კავშირისას, ქსელის გამტარუნარიანობა და ნდობა შესაძლოა არ იყოს საკმარისი კონკრეტულ ან სხვა არეალში. მეორე მხრივ, შესაძლებელია დასაბუთებულად ვივარაუდოთ, რომ დახურული ღრუბლოვანი სისტემები გაქირავდეს ზემოხსენებულ შემთხვევებში (აღმოჩნდეს მეტად ეკონომიური), ან ასევე შესაძლოა დაინერგოს ჰიბრიდული მოდელებიც (დახურული და საჯარო კომპონენტების გათვალისწინებით). ყველა შემთხვევაში, შესაბამისი სავარაუდო შედეგები უნდა გავითვალისწინოთ.

საერთაშორისოდ აღიარებული სტანდარდების არარსებობისას, ღრუბლოვანი სისტემების მიერ წარმოიშობა ე.წ „თავად მოაწესრიგე“-ს რისკი, ასევე, გაერთიანებული ღრუბლოვანი მოდიფიკაციები, რომელიც მოიცავს ბლოკირების საფრთხეებს (წოდებული როგორც პრივატულ მონოკულტურად)[51] და ახდენს მთლიანი კონტროლის პრევენციას მონაცემებზე, ჩარევაუნარიანობის უზრუნველყოფის გარეშე. მონაცემთა პორტატულობა და ჩარევაუნარიანობა საკვანძო საკითხებს წარმოადგენს ღრუბლოვან სისტემაზე

51 იხ. ევროპული პარლამენტის კვლევა “Does it Help or Hinder? Promotion of Innovation on the Internet and Citizens’ Right to Privacy”, გამოქვეყნებული 2011 წლის დეკემბერში.

დაფუძნებული ტექნოლოგიის განვითარებისთვის, ასევე, მონაცემთა სუბიექტების მიერ მონაცემთა დაცვიდან გამომდინარე უფლებების რეალიზაციისთვის (როგორიცაა წვდომა და შესწორება).

ამ მსჯელობის შედეგად, ღრუბლოვან ტექნოლოგიებზე არსებული დებატი წარმოადგენს მნიშვნელოვან მაგალითს იმ დაპირისპირებისა, რომელიც არსებობს ეკონომიურ და უფლებადაცვით მიდგომებთან დაკავშირებით, რაც მეორე ნაწილში მოკლედ იქნა მიმოხილული. დახურულ ღრუბლოვან სისტემაზე დაყრდნობა შესაძლებელია მისაღები და რეკომენდირებული იყოს მონაცემთა დაცვის პერსპექტივიდან გამომდინარე, დამუშავების განსაკუთრებული პირობების გათვალისწინებით, თუმცა არ იყოს პრაქტიკული იმ ორგანიზაციებისთვის, რომელიც ფუნქციონირებენ ეკონომიური მიდგომის პერსპექტივიდან. აუცილებელია მოცემული ინტერესების ფრთხილი ანალიზი, ვინაიდან ამ მხრივ, ერთი კონკრეტული მიდგომა ვერ დადგინდება.

გამომცემლობა „იურისტების სამყარო“

თბილისი, მ. კოსტავას ქ. №75

ტელ:. 238 35 99; 557 51 51 34

ელ-ფოსტა: Lawyers.world@yahoo.com;

ვებ-გვერდი: www.law.ge

https://www.facebook.com/PublishingHouselawyersworld