ნორბერტ ბერნსდორფი*

პერსონალური მონაცემების გადაცემა მესამე სახელმწიფოებში - „უსაფრთხო ნავსადგომი“, „ევროკავშირი-აშშ-ს პირადი ცხოვრების დამცავი სისტემა“ და „ტრანსატლანტიკური მონაცემთა კონფიდენციალობის ჩარჩო“

ახალი შეთანხმება - “ტრანსატლანტიკური მონაცემთა კონფიდენციალობის დამცავი სისტემა” („Trans-Atlantic Data Privacy Shield Framework“) წარმოადგენს “ევროკავშირი-აშშ-ს პირადი ცხოვრების დამცავი სისტემის” (“EU-US Privacy Shield”) შეთანხმების სამართალმემკვიდრეს. *ევროკომისიის შესაბამისობის გადაწყვეტილება, რომელიც ამ უკანასკნელს ეფუძნებოდა, ევროკავშირის მართლმსაჯულების სასამართლოს (“CJEU”) სენსაციური გადაწყვეტილებით („Schrems II“), 2020 წლის ივლისში გამოცხადდა ძალადაკარგულად. აღნიშნულს წინ უძღოდა შესაბამისობის გადაწყვეტილების კრიტიკა ლუქსემბურგის მოსამართლეების მხრიდან, რაც „უსაფრთხო ნავსადგომის“ სახელით ცნობილი შეთანხმებიდან გამომდინარეობდა. ორივე შემთხვევა შეეხებოდა აშშ-ს უსაფრთხოების სამსახურების ფართო უფლებამოსილებას ევროკავშირის მოქალაქეების პერსონალურ მონაცემებთან მიმართებაში. “CJEU”-მ დაადგინა, რომ აშშ-ში მონაცემთა დაცვის დონე არ შეესაბამებოდა ევროკავშირის სტანდარტებს.*

საკვანძო სიტყვები: *მონაცემთა კონფიდენციალობა, მონაცემთა დაცვა, მესამე სახელმწიფოებისათვის გადაცემა, „უსაფრთხო ნავსადგომის“ შეთანხმება, „ევროკავშირი-აშშ-ს პირადი ცხოვრების დამცავი სისტემა“, „ტრანსატლანტიკური მონაცემთა კონფიდენციალობის ჩარჩოს“ შეთანხმება, “Facebook”, ევროკავშირის მართლმსაჯულების სასამართლო, პრეცედენტული სამართალი, მონაცემთა დაცვის ძირითადი რეგულაცია (“GDPR”).*

* მარბურგის ფილიპეს სახელობის უნივერსიტეტის პროფესორი, სამართლის დოქტორი; გერმანიის სოციალურ საკითხთა ფედერალური სასამართლოს ყოფილი მოსამართლე, წინამდებარე ჟურნალის სარედაქციო კოლეგიის წევრი.

1. შესავალი

პერსონალური მონაცემები, შესაძლოა, გადაეცეს მესამე სახელმწიფოს მხოლოდ იმ შემთხვევაში, თუ გარანტირებულია „მონაცემთა დაცვის ძირითადი რეგულაციით“ (“GDPR”)[1] დადგენილი სტანდარტი. მესამე სახელმწიფოებად იწოდებიან ქვეყნები, სადაც “GDPR” არ გამოიყენება. იქიდან გამომდინარე, რომ “GDPR” სავალდებულოა მხოლოდ ევროკავშირის (“EU”) წევრი ქვეყნებისთვის, მესამე სახელმწიფოებად მოიხსენიება ევროკავშირის არაწევრი ქვეყნები. ევროპული ეკონომიკური ზონის (“EEA”) ქვეყნები, მაგალითად, ისლანდია, ლიხტენშტეინი და ნორვეგია, ასევე, მიეკუთვნებიან მესამე სახელმწიფოების ჯგუფს, თუ ისინი თავად არ გადაწყვეტენ, შეუერთდნენ “GDPR”-ს. მონაცემთა გადაცემის სერიოზული პრობლემა არსებობს ამერიკის შეერთებულ შტატებში (აშშ), რადგან აშშ-ში მონაცემთა დაცვის ევროპის მსგავსი დონე არ არის უზრუნველყოფილი.

„ედვარდ სნოუდენის საქმისა” და საიდუმლო სამსახურის მხრიდან მასობრივი თვალთვალის გამოვლენის გათვალისწინებით, აშშ-ში მონაცემთა დაცვის მიმართ ნდობა დაიკარგა. აშშ-ში შესაძლებელია, განხორციელდეს ევროკავშირის მოქალაქეების მონიტორინგი მაშინაც კი, როდესაც ისინი აგზავნიან შეტყობინებებს სოციალური ქსელის, “Facebook”-ის (“Meta”) მეშვეობით.

მას შემდეგ, რაც მონაცემთა დაცვის შესახებ შეთანხმებები - „უსაფრთხო ნავსადგომი“ და „ევროკავშირი-აშშ-ის კონფიდენციალობის ჩარჩო“ - გააუქმა ევროკავშირის მართლმსაჯულების სასამართლომ, ევროკავშირი და აშშ უკვე მესამედ ცდილობენ მონაცემთა დაცვის ევროპული სტანდარტები შეუსაბამონ აშშ-ს სათვალთვალო პრაქტიკას.

2. ისტორია და მნიშვნელობა

მონაცემთა დაცვის ადრე მოქმედი დირექტივით (95/46/EC; DPD)[2], მართებულად იყო აღიარებული მონაცემთა ტრანსსასაზღვრო გადაადგილება, როგორც საერთაშორისო ვაჭრობის განვითარების აუცილებლობა. მონაცემთა ტრანსსასაზღვრო ნაკადი და, შესაბამისად, პერსონალური მონაცემების ტრანსსასაზღვრო გადაცემა, უდავოდ, ციფრული სამყაროს გამოწვევაა. თუმცა, მსოფლიოში არ არსებობს და არც შეიძლება არსებობდეს მონაცემთა დაცვის თანაბარი დონე ან თუნდაც მონაცემთა დაცვის თანაბარი კონცეფცია[3].

მონაცემთა დაცვის დირექტივას ორი მთავარი დანიშნულება ჰქონდა: ერთი მხრივ, შეიქმნა მონაცემთა დაცვის ეროვნული კანონმდებლობის ჩარჩო ევროკავშირის მასშტაბით, რითაც განხორციელდა მონაცემთა დაცვის დონის ჰარმონიზაცია და ჩამოყალიბდა ერთგვარი ჩარჩო პირობები ევროკავშირის შიგნით პერსონალური მონაცემების შეუფერხებელი გადაცემისთვის, მეორე მხრივ კი, მონაცემთა დაცვის თვალსაზრისით, ევროკავშირი გაიმიჯნა სხვა ქვეყნებისაგან,

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, OJ 2016 L 119, 1.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281, 31.

[3] *იხ.: Wuermeling U.*, Handelshemmnis Datenschutz - Die Drittländerregelung der Europäischen Datenschutzrichtlinie, Berlin, 2000.

რამდენადაც ითვალისწინებდა პირობებს, რომლებითაც მონაცემების გადაცემა ევროკავშირის წევრ ქვეყნებთან ერთად, შესაძლებელი გახდა სხვა ქვეყნებშიც.

ზემოაღნიშნული მიდგომა გაზიარებულია “GDPR”-ის 44-ე - 50-ე მუხლებშიც, თუმცა, აღსანიშნავია, რომ ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაცია“ საგრძნობლად გასცდა დირექტივის დებულებების სიღრმეს. “GDPR”, 1995 წლიდან მოყოლებული, ეხმიანება მონაცემთა დაცვის სფეროში განვითარებულ მოვლენებს. მნიშვნელოვანია ისიც, რომ, მიუხედავად ევროკავშირის მონაცემთა დაცვის კანონმდებლობის მიზნისა, დაიცვას პერსონალური მონაცემები, მან არ უნდა შეაფერხოს ეკონომიკური ზრდა.[4] მესამე სახელმწიფოებთან მონაცემთა ტრანსსასაზღვრო გადაცემას გადამწყვეტი მნიშვნელობა აქვს ბიზნესისა და ვაჭრობისთვის, თუმცა, ამასთანავე, წარმოქმნის მონაცემთა დაცვის რისკებს.

3. ევროკავშირის „მონაცემთა დაცვის ძირითადი რეგულაციის“ სისტემა

პერსონალური მონაცემების მესამე სახელმწიფოსთვის გადაცემა რეგულირდება “GDPR”-ის 44-ე - 50-ე მუხლებით, რაც ქმნის მონაცემთა დაცვის ერთიან სტანდარტს ევროკავშირის ფარგლებში. იმავდროულად, აღნიშნული მესამე სახელმწიფოებში პერსონალური მონაცემების დამუშავების შეზღუდვების დაწესებით, განასხვავებს ევროკავშირს სხვა ქვეყნებისგან.

“GDPR”-ის 44-ე მუხლი ადგენს პერსონალური მონაცემების მესამე სახელმწიფოსთვის გადაცემის ზოგად პრინციპებს. 45-ე - 49-ე მუხლები ასახავს ამგვარი გადაცემის ლეგიტიმაციის სხვადასხვა მექანიზმს და დასაშვებობის კრიტერიუმებს, რომლებიც იურიდიულად ერთმანეთთან დაკავშირებული არ არის. 45-ე მუხლის თანახმად, მონაცემთა გადაცემის საფუძველია მონაცემთა დაცვის შესაბამისობის გადაწყვეტილება. პერსონალური მონაცემების ინდივიდუალური კონკრეტული გადაცემა ნებადართულია “GDPR”-ის 48-ე და 49-ე მუხლების საფუძველზე; 50-ე მუხლი კი შეეხება საერთაშორისო თანამშრომლობას პერსონალურ მონაცემთა დაცვის სფეროში.

პერსონალური მონაცემების მესამე სახელმწიფოსათვის გადაცემის დასაშვებობის შეფასება მოითხოვს ორეტაპიან შემოწმებას.[5] რეგულაციის 44-ე მუხლი განმარტავს, რომ გარდა მეხუთე თავით დადგენილი წესებისა, გადაცემა შესაბამისობაში უნდა იყოს “GDPR”-ის სხვა დებულებებთანაც, მათ შორის, მე-6, მე-9 და მე-10 მუხლებთან.[6] საწყის ეტაპზე, “GDPR”-ის მე-6, მე-9 და მე-10 მუხლებში ასახული ზოგადი აკრძალვისა და გამონაკლისების შესაბამისად, აუცილებელია, დადგინდეს, არსებობს თუ არა კანონიერი საფუძველი მონაცემთა გადაცემისთვის. მეორე ეტაპზე კი, აუცილებელია იმის შემოწმება, არის თუ არა დაცული “GDPR”-ის 44-ე და მომდევნო მუხლებით დადგენილი მოთხოვნები. მხოლოდ ამ პირობების

[4] For more information see: *Rüpke G.*, *von Lewinski K., Eckardt J. (eds.)*, Datenschutzrecht - Grundlagen und europarechtliche Umgestaltung, München 2018, § 18. On the requirements of a "European internal data market" *Brink St.*, *Oetjen St.*, *Schwartmann R.*, *Voss K.*, So war die DSGVO nicht gemeint, Frankfurter Allgemeine Zeitung (FAZ) v. 17 July 2022.

[5] Likewise: *Albrecht J. Ph.*, *Jotzo Fl.*, Das neue Datenschutzrecht der Europäischen Union, Baden-Baden, 2017, Part 6.

[6] *Schantz P.*, *Wolff H. A.*, Das neue Datenschutzrecht, Berlin, 2017, 239.

დაკმაყოფილების შემთხვევაში არის ნებადართული პერსონალური მონაცემების მესამე სახელმწიფოსათვის გადაცემა. აღნიშნული ორსაფეხურიანი სტრუქტურა გამომდინარეობს "GDPR"-ის მიზნიდან და სისტემიდან. ის ქმნის მონაცემთა დაცვის სამართლებრივ ჩარჩო სტანდარტს ევროკავშირში. შესაბამისად, ტრანსსასაზღვრო დამუშავება, როგორც ასეთი, არ წარმოადგენს რისკს მონაცემთა სუბიექტისთვის. რისკი წარმოიქმნება მაშინ, როდესაც პერსონალური მონაცემები გადაეცემა მონაცემთა დამუშავებაზე პასუხისმგებელი ერთი პირიდან მეორეს. სწორედ "GDPR"-ის მე-6, მე-9 და მე-10 მუხლები ითვალისწინებს ზემოხსენებულ რისკს,[7] დამატებით რისკს კი წარმოადგენს მონაცემთა გადაცემა ჰარმონიზებული საკანონმდებლო ბაზის ფარგლებს მიღმა.

მონაცემთა გადაცემა მესამე სახელმწიფოებს შორის დასაშვებია მხოლოდ იმ შემთხვევაში, თუ დაცული იქნება "GDPR"-ის წესები, მათ შორის, 44-ე და შემდგომი მუხლები.

4. ევროკავშირის მართლმსაჯულების სასამართლოს პრეცედენტული სამართალი

პერსონალური მონაცემების აშშ-ში გადაცემა არაერთხელ იქნა გაკრიტიკებული ევროკავშირის მართლმსაჯულების სასამართლოს მიერ. თავდაპირველად, მან ძალადაკარგულად გამოაცხადა ევროკავშირისა და აშშ-ს „უსაფრთხო ნავსადგომის" შეთანხმება, შემდეგ კი, „ევროკავშირი-აშშ-ის კონფიდენციალობის ფარის" შეთანხმება და მასთან დაკავშირებული ევროკომისიის შესაბამისობის გადაწყვეტილებები.

ა. ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილება საქმეზე C-362/14, Maximillian Schrems/Data Protection Commissioner, Digital Rights Ireland Ltd, 2015 წლის 6 ოქტომბერი ("Schrems I")[8]

„ევროკომისიის უსაფრთხო ნავსადგომის პრინციპების შესახებ" ევროკავშირის მართლმსაჯულების სასამართლოს 2015 წლის 6 ოქტომბრის გადაწყვეტილებით, რომელსაც უდიდესი მნიშვნელობა ჰქონდა, დადგინდა მონაცემთა დაცვის ადრე მოქმედი დირექტივის (DPD) ფუნდამენტური პრინციპები. მან, ასევე, მნიშვნელოვანი გავლენა იქონია "GDPR"-ის 44-ე - 50-ე მუხლების შინაარსის ჩამოყალიბებაზე.

საქმის ფაქტობრივი გარემოებები: შრემსი იყო ავსტრიის მოქალაქე, რომელმაც საჩივარი შეიტანა ირლანდიის მონაცემთა დაცვის საზედამხედველო ორგანოში იმის გამო, რომ მისი პერსონალური მონაცემები "Facebook"-ის ადგილობრივმა შვილობილმა კომპანიამ გადასცა "Facebook Inc."-ს და აშშ-ში მდებარე სერვერებს, სადაც მუშავდებოდა ასეთი მონაცემები. იმ დროს, ევროკავშირის ტერიტორიაზე მცხოვრებ "Facebook"-ის ყველა მომხმარებელს რეგისტრაციისას უნდა გაეფორმებინა ხელშეკრულება "Facebook Ireland"-თან, რის გამოც, ევროკავშირის ტერიტორიაზე მცხოვრები "Facebook"-ის მომხმარებლების პერსონალური მონაცემები სრულად ან ნაწილობრივ გადაეცემოდა აშშ-ში მდებარე "Facebook Inc."-

[7] იხ.: *Rüpke G., von Lewinski K., Eckardt J. (eds.)*, Datenschutzrecht- Grundlagen und europarechtliche Umgestaltung, München, 2018, § 18, 266.
[8] ECLI:EU:C:2015:650.

ის სერვერებს. ირლანდიის მონაცემთა დაცვის საზედამხედველო ორგანომ საჩივარი მიიჩნია უსაფუძვლოდ, არ მიიღო და განმარტა, რომ მონაცემთა აშშ-სთვის გადაცემა ეფუძნებოდა 2000 წელს მიღებულ შესაბამისობის კომისიის გადაწყვეტილებას 2000/520/EC[9] და იძლეოდა მონაცემთა გადაცემის ნებართვას ამერიკულ კომპანიებზე, რომლებიც აცხადებდნენ, რომ დაიცავდნენ ევროკავშირიდან მიღებულ პერსონალურ მონაცემებს და შეასრულებდნენ ე.წ. „უსაფრთხო ნავსადგომის” პრინციპებს.

ამდენად, ირლანდიის მონაცემთა დაცვის საზედამხედველო ორგანომ მიიჩნია, რომ ვალდებული იყო, საჩივრის განხილვის გარეშე სრულად გაეზიარებინა ევროკომისიის შესაბამისობის გადაწყვეტილება, რის შემდეგაც შრემსმა გადაწყვეტილება სასამართლოში გაასაჩივრა.

ირლანდიის უმაღლესმა სასამართლომ შეშფოთება გამოხატა აშშ-ში მონაცემთა გადაცემის დასაშვებობასთან დაკავშირებით და საკითხი მოსაკვლევად და წინასწარი განჩინების გამოსატანად გადასცა ევროკავშირის მართლმსაჯულების სასამართლოს, კომისიის გადაწყვეტილების იურიდიული ძალის განსაზღვრისა და მისი ევროკავშირის ფუნდამენტურ უფლებათა ქარტიის[10] მე-8 მუხლთან შესაბამისობის დადგენის მიზნით.

ირლანდიის უმაღლესი სასამართლო ევროკომისიის 2000/520/EC გადაწყვეტილების კანონიერების საკითხის განხილვისას „უსაფრთხო ნავსადგომის” პრინციპებს არ შეხებია, თუმცა, მიუხედავად ამისა, “CJEU”-მ საბოლოოდ მაინც იმსჯელა აღნიშნულ საკითხზე, რადგან შრემსის საჩივარი ფაქტობრივად ეჭვქვეშ აყენებდა გადაწყვეტილების კანონიერებასაც. შედეგად, “CJEU”-მ გააფართოვა გადაწყვეტის ფარგლები.

“CJEU”-მ დაადგინა, რომ მონაცემთა დაცვის საზედამხედველო ორგანოებს, დირექტივის (DPD) მიხედვით, ევროკომისიის გადაწყვეტილებების დამოუკიდებლად გადახედვის უფლებამოსილება გააჩნიათ, მიუხედავად იმისა, რომ მხოლოდ “CJEU”-ს შეუძლია ევროკომისიის გადაწყვეტილებების ბათილად გამოცხადება. შესაბამისად, იმ შემთხვევაშიც კი, როდესაც პერსონალურ მონაცემთა გადაცემის საფუძველია კომისიის გადაწყვეტილება შესაბამისობაზე, ეროვნულ საზედამხედველო ორგანოში საჩივრის შეტანისას, უწყება ვალდებულია, გულმოდგინედ განიხილოს მოთხოვნა.

ევროკავშირის მართლმსაჯულების სასამართლომ სიტყვასიტყვით განაცხადა:

„კანონმდებლობა, რომელიც საჯარო ხელისუფლებას აძლევს ელექტრონულ კომუნიკაციებზე ფართო წვდომის საშუალებას, ძირს უთხრის პირადი ცხოვრების ხელშეუხებლობის ფუნდამენტურ უფლებას, რომელიც დაცულია ქარტიის მე-7 მუხლით (იხ.: გადაწყვეტილება Digital Rights Ireland and Others, C-293/12 და C-594/12, ECLI:EU:C:2014:238, § 39).

ანალოგიურად, კანონმდებლობა, რომელიც არ ითვალისწინებს ინდივიდის შესაძლებლობას, გამოიყენოს სამართლებრივი დაცვის საშუალებები, რათა ჰქონდეს წვდომის, შესწორების და წაშლის უფლება პირადად მასთან დაკავშირებულ პერსონალურ მონაცემებზე, არღვევს ქარტიის 47-ე მუხლის საფუძველზე ეფექტიანი სასამართლოს უფლების არსს. ქარტიის 47-ე მუხლის პირველი პუნქტით დადგენილია, რომ ევროკავშირის კანონმდებლობით გარანტირებული უფლებებისა და

[9] Decision 2000/520/EC of the European Commission of 26 July 2000.
[10] Charter of Fundamental Rights of the European Union, OJ 2010 L 83, 389.

თავისუფლებების დარღვევის შემთხვევაში, პირს სამართლებრივი დაცვის ეფექტიანი საშუალების მოთხოვნის უფლება აქვს, ამ მუხლით გათვალისწინებული პირობების დაცვით. ეფექტიანი სასამართლო განხილვის შესაძლებლობა უზრუნველყოფს ევროკავშირის კანონმდებლობის დაცვას, რაც აუცილებელია კანონის უზენაესობისთვის. (...).“

მართლმსაჯულების ევროპულმა სასამართლომ, თავისი გადაწყვეტილებით, არამხოლოდ ძალადაკარგულად ცნო ევროკავშირსა და აშშ-ს შორის „უსაფრთხო ნავსადგომის“ შეთანხმება, არამედ დაადგინა მონაცემთა დაცვის დონის შესაბამისობის შეფასების კრიტერიუმები.[11] აღნიშნულმა გავლენა იქონია ძალადაკარგული შეთანხმების სამართალმემკვიდრეზეც - "ევროკავშირი-აშშ-ის კონფიდენციალობის ფარი"-ზე რომელიც მოექცა გაძლიერებული კონტროლის ქვეშ მონაცემთა დაცვის კანონმდებლობისა და შესაბამისი პოლიტიკის თვალსაზრისით.

ბ. ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილება საქმეზე C-311/18, Data Protection Commissioner/Facebook Ireland Ltd, Maximillian Schrems, 16 July 2020 ("Schrems II")[12]

აშშ-ში მონაცემთა მიმოცვლის მნიშვნელობის ხაზგასასმელად, 2016 წლის 12 ივლისს “EU-US Privacy Shield” - შეთანხმება იქნა მიღწეული, რომელიც „უსაფრთხო ნავსადგომის“ სამართალმემკვიდრედ მიიჩნევა. შეთანხმება ევროკომისიის შესაბამისობის გადაწყვეტილებას 2016/1250 დაეფუძნა,[13] რომლის მიხედვით, ორგანიზაციები, რომლებმაც ნებაყოფლობით აიღეს “EU-US Privacy Shield” მექანიზმის იმპლემენტაციის ვალდებულება, პასუხისმგებელნი არიან, უზრუნველყონ მონაცემთა დაცვის შესაბამისი დონე.

„ევროკავშირი-აშშ-ის კონფიდენციალურობის ფარი“ ადრინდელი „უსაფრთხო ნავსადგურის“ შეთანხმების მსგავსი იყო. ამერიკულმა კომპანიებმა აშშ-ს ვაჭრობის დეპარტამენტის წინაშე ნებაყოფლობით აიღეს ვალდებულება, ევროკავშირიდან გადაცემული მონაცემები მხოლოდ დადგენილი პრინციპების შესაბამისად დაემუშავებინათ, რათა შენარჩუნებულიყო ევროკავშირის მონაცემთა დაცვის დონე. ფედერალური სავაჭრო კომისია და აშშ-ის სატრანსპორტო დეპარტამენტი ზედამხედველობას უწევდნენ ვალდებულებების შესრულებას „ევროკავშირი-აშშ-ის კონფიდენციალურობის ფარის“ ფარგლებში. ვაჭრობის დეპარტამენტი უმთავრესად პასუხისმგებელი იყო ნებაყოფლობითი ვალდებულების შესრულების მონიტორინგზე, ხოლო ფედერალურ სავაჭრო კომისიას შეეძლო ორგანიზაციების დაჯარიმება. თუმცა, თავიდანვე არსებობდა ეჭვი იმის თაობაზე, თუ რამდენად ეფექტიანად შეძლებდა აშშ-ს ხელისუფლება მონაცემთა დაცვის ზედამხედველობასა და აღსრულებას.

საქმის ფაქტობრივი გარემოებები: „უსაფრთხო ნავსადგომის“ საქმეში, მოქალაქე შრემსმა საჩივარი შეიტანა ირლანდიის მონაცემთა დაცვის ორგანოში, იგი მიუთითებდა, რომ “Facebook Ireland” გადასცემდა მის პერსონალურ მონაცემებს აშშ-ს. ირლანდიის სასამართლომ ევროკავშირის მართლმსაჯულების სასამართლოს მიმართა ხელშეკრულების სტანდარტული პირობებისა და „ევროკავშირი-აშშ-ის კონფიდენციალურობის ფარი“-ს შესაბამისობის დასადგენად ევროკავშირის

[11] Likewise *Kühling J.*, *Heberlein J.*, EuGH "reloaded": "unsafe harbour" USA vs. "Datenfestung" EU, Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2016, 7,9.

[12] ECLI:EU:C:2020:559.

[13] Decision (EU) 2016/1250 of the European Commission of 12 July 2016.

მონაცემთა დაცვის სტანდარტებთან. “CJEU”-მ დაადგინა, რომ „ევროკავშირი-აშშ-ის კონფიდენციალურობის ფარი“ არ იყო დამაკმაყოფილებელი ევროკავშირის სტანდარტებთან მიმართებით. გარდა ამისა, ფიზიკური პირებისთვის ხელმისაწვდომი სამართლებრივი დაცვა, როგორიცაა ეფექტიანი სამართლებრივი დაცვის უფლება, არასაკმარისად იქნა მიჩნეული.

ამ მოვლენების შემდეგ მნიშვნელოვანი საკითხი იყო აშშ-ს ხელისუფლების შესაძლებლობა, მიეღო წვდომა ევროკავშირიდან გადაცემულ მონაცემებზე და შეზღუდული სამართლებრივი საშუალებები, რომლებიც ხელმისაწვდომი იყო ამგვარი წვდომის გასაჩივრების მიზნით. აღნიშნულის გამო “CJEU”-მ მიიღო გადაწყვეტილება „უსაფრთხო ნავსადგომის“ მექანიზმის ბათილად ცნობის შესახებ.

“CJEU”-მ განმარტა:

„აშშ-ს კანონმდებლობით პერსონალური მონაცემების დაცვის შეზღუდვები, განსაკუთრებით აშშ-ს საჯარო ხელისუფლების მიერ ევროკავშირის მიერ გადაცემული მონაცემების ხელმისაწვდომობასა და გამოყენებასთან დაკავშირებით, არ აკმაყოფილებს ევროკავშირის კანონმდებლობით დადგენილ მოთხოვნებს, როგორც მითითებულია ევროკავშირის ძირითად უფლებათა ქარტიის 52(1) მუხლის მეორე წინადადებაში. კანონმდებლობა, რომელიც ფიზიკურ პირს არ აძლევს სამართლებრივი დაცვის საშუალებათა გამოყენების შესაძლებლობას - ჰქონდეს ხელმისაწვდომობა მის შესახებ არსებულ პერსონალურ მონაცემებზე, ან მოითხოვოს ასეთი მონაცემების შესწორება ან წაშლა - არ შეესაბამება ეფექტიანი სამართლებრივი დაცვის ფუნდამენტურ უფლებას (ქარტიის 47-ე მუხლი).“ ამრიგად, „უსაფრთხო ნავსადგომის გადაწყვეტილებით“, აშშ ვერ დაიცავდა ფუნდამენტურ უფლებებს იმ დონეზე, რომელიც გარანტირებულია ევროკავშირის დირექტივით, ქარტიასთან ერთობლიობაში. შესაბამისად, “CJEU”-მ გადაწყვეტილება გამოაცხადა ძალადაკარგულად“.

რა როლს ასრულებენ ევროკომისია და მონაცემთა დაცვის ეროვნული საზედამხედველო ორგანოები მესამე ქვეყნებისთვის მონაცემთა გადაცემისას?

ევროკომისიას არ მოეთხოვება მესამე ქვეყნებში მონაცემთა დაცვის დონის შეფასება, სტანდარტულ სახელშეკრულებო პუნქტების მიღებისას. ევროკავშირის მართლმსაჯულების სასამართლო ხაზს უსვამს, რომ მონაცემთა გამცემის (ექსპორტიორის) პასუხისმგებლობაა მესამე ქვეყანაში მონაცემთა დაცვის დონის შეფასება თითოეული გადაცემისთვის. მონაცემთა გამცემმა ასევე უნდა უზრუნველყოს ადეკვატური დაცვა შესაბამისი გარანტიებით, რომელიც შეიძლება მოიცავდეს დამატებით ზომებს ხელშეკრულების სტანდარტული პირობების მიღმა.

თუ მონაცემთა დაცვა ვერ იქნება უზრუნველყოფილი დამატებითი ზომებითაც კი, მონაცემთა გამცემმა უნდა შეაჩეროს ან შეწყვიტოს მონაცემთა გადაცემის პროცესი.

მონაცემთა დაცვის ეროვნულ საზედამხედველო ორგანოებს აქვთ ძალიან მნიშვნელოვანი როლი დაცვის გარანტიების ზედამხედველობის კუთხით, როგორიცაა ხელშეკრულების სტანდარტული პირობები. ორგანოებმა უნდა გადახედონ ამ გარანტიებს, განსაკუთრებით მაშინ, როდესაც საჩივარი ეჭვქვეშ აყენებს ევროკომისიის შესაბამისობის გადაწყვეტილების ეფექტიანობას მონაცემთა გადაცემასთან მიმართებით

“GDPR”-ის 58-ე მუხლის თანახმად, ეროვნულმა საზედამხედველო ორგანოებმა უნდა აკრძალონ ან შეაჩერონ მონაცემთა გადაცემა, თუ არ არსებობს ევროკომისიის

მოქმედი შესაბამისობის გადაწყვეტილება, ან ადეკვატური გარანტია ან/და დამატებითი ზომები საკმარისად არ უზრუნველყოფს მესამე ქვეყანაში გადაცემული მონაცემების დაცვას.

მესამე ქვეყნისთვის მონაცემთა გადაცემისას მონაცემთა დაცვის დონის შეფასების მიზნით საზედამხედველო ორგანოებმა უნდა იხელმძღვანელონ ევროკომისიის შესაბამისობის გადაწყვეტილებებით, როდესაც ეს უკანასკნელი ძალაშია.

5. ახალი „ტრანსატლანტიკური მონაცემთა კონფიდენციალობის ჩარჩო“ შეთანხმება

ევროკავშირის მართლმსაჯულების სასამართლოს 2020 წლის 16 ივლისის გადაწყვეტილების შემდეგ („შრემს II“), ევროკავშირის კომისია და აშშ კვლავ ცდილობდნენ შეემუშავებინათ მონაცემთა დაცვის შესახებ ახალი შეთანხმება. ახალი შესაბამისობის გადაწყვეტილების მიზანია ამერიკულ ორგანიზაციებში პერსონალური მონაცემების უსაფრთხო გადაცემის უზრუნველყოფა.

ა. მომზადების პროცესი

2022 წლის 25 მარტს აშშ-ს პრეზიდენტმა ბაიდენმა და ევროკომისიის პრეზიდენტმა ფონ დერ ლაიენმა გამოაცხადეს შეთანხმება „ტრანსატლანტიკური მონაცემთა კონფიდენციალურობის ფარის ჩარჩოზე“. ამ შეთანხმების დეტალები სხვა წყაროებთან ერთად გაზიარებული იყო აშშ-ს მთავრობის პრესრელიზში.[14]

აღნიშნული იწვევს შემდეგს:[15]

„ევროკავშირი-აშშ-ის კონფიდენციალურობის ფარის“ - შეთანხმების ომბუდსმენის ნაცვლად, „ტრანსატლანტიკური მონაცემთა კონფიდენციალურობის ფარი“ - შეთანხმება არის კვაზი-სასამართლო, ორსაფეხურიანი ორგანო, რომელიც ევროკავშირის მასშტაბით მონაცემთა სუბიექტების საჩივრებს განიხილავს. ორგანო უფლებამოსილია, შექმნას სამართლებრივი დაცვის საშუალებები. მიუხედავად იმისა, რომ ის არ უნდა იყოს სასამართლო სისტემის ნაწილი, უნდა იყოს დამოუკიდებელი და აშშ-ს მთავრობის წევრებით არ დაკომპლექტდნენ.

გარდა ამისა, ახალი ზომები მტკიცდება აშშ-ს უსაფრთხოების ორგანოებში, რათა შემცირდეს თვალთვალი პროპორციულ დონეზე და განხორციელდეს კონსტიტუციური სტანდარტები, თუმცა დეტალები ჯერ კიდევ უცნობია. ცვლილებები არ განხორციელდება კონგრესის მიერ მიღებული კანონით, არამედ აშშ-ს პრეზიდენტის მიერ გამოცემული ახალი ადმინისტრაციული წესით (აღმასრულებელი ბრძანება).

---

[14] For more information see: <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states and european commission-announce-trans-atlantic-data-privacy-shield framework.pdf> [10.05.2024]. Also *Glocker F.*, Politische Lösung für Datentransfers in die USA zeichnet sich ab <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/trans-atlantic-data-privacy-shield-framework.html> [10.05.2024].

[15] *Glocker F.,* EU-US Data Privacy Framework: Beschluss der EU-Kommission, <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/eu-us-data-privacy-framework-beschluss-der-eu-kommission.html> [10.05.2024] Also: *Glocker F.,* Politische Lösung für Datentransfer in die USA zeichnet sich ab <https://www.cmshs-bloggt.de/datenschutzrecht/trans-atlantic-data-privacy-shield-framework.html> [10.05.2024].

„Trans-Atlantic Data Privacy Shield Framework“ ეფუძნება წინა „EU-US Privacy Shield“ მექანიზმს. ამერიკული კომპანიებისთვის მოთხოვნები უცვლელი დარჩება და არსებული სერტიფიკატები კვლავ ძალაში დარჩება, ხოლო ტერმინი „კონფიდენციალურობის ფარი“ კვლავაც იქნება გამოყენებული სერტიფიცირების მიზნებისთვის. აღსანიშნავია, რომ აშშ-ს მთავრობამ "კონფიდენციალურობის ფარის" სერტიფიკატი 2020 წლის 16 ივლისის ევროკავშირის მართლმსაჯულების სასამართლოს გადაწყვეტილების შემდეგაც კი შეინარჩუნა.[16]

"Trans-Atlantic Data Privacy Shield Framework" - შეთანხმება შეიცავს გარკვეულ პრინციპებს ამერიკული კომპანიების თვითსერტიფიკაციისთვის, რომლებიც ეფუძნება მონაცემთა დაცვის ევროპულ კანონს. აღნიშნული პრინციპები განიხილება, როგორც “GDPR”-ის გამარტივებულ ვერსია[17]. თვითსერტიფიკაცია გულისხმობს სარეგისტრაციო მოსაკრებლის გადახდის გზით ამერიკული კომპანიის დარეგისტრირებას კომერციის დეპარტამენტის ვებგვერდზე. აღნიშნული ვებგვერდი ხელმისაწვდომია 2023 წლის 17 ივლისიდან.[18] აქედან მოყოლებული, დაახლოებით 2600 ამერიკული კომპანია, რომელიც ადრე იყო სერტიფიცირებული „კონფიდენციალურობის ფარის“ ფარგლებში, ავტომატურად იქნება აღიარებული სერტიფიცირებულად „ტრანსატლანტიკური მონაცემთა კონფიდენციალურობის ჩარჩოს“ მიხედვით. მათ შორისაა: აშშ-ს ძირითადი “Cloud Provider” - SaaS და IT სერვისის მიმწოდებლები.

ბ. ე.წ. ევროკომისიის აღმასრულებელი ბრძანება და შესაბამისობის გადაწყვეტილება

2023 წლის 10 ივლისს ევროკავშირის კომისიამ მიიღო “Trans-Atlantic Data Privacy Shield Framework” - შეთანხმება და შესაბამისობის გადაწყვეტილება[19]. აშშ-ის მთავრობამ ასევე გამოაქვეყნა აშშ-ის პრეზიდენტის ე.წ. აღმასრულებელი ბრძანება. იმ შემთხვევაში თუ აშშ-ს კომპანიები გაივლიან თვითსერტიფიკაციას ახალი მექანიზმით, ივარაუდება, რომ უზრუნველყოფილია მონაცემთა დაცვის შესაბამისი სტანდარტი.[20]

6. დასკვნა - "Schrems III"?

"Trans-Atlantic Data Privacy Shield Framework"- შეთანხმებას აქვს გადამწყვეტი უპირატესობა: ის სამართლებრივ უსაფრთხოებას უზრუნველყოფს. ევროკომისიის ახალი შესაბამისობის გადაწყვეტილება ავალდებულებს მონაცემთა დაცვის

[16] For more information see: <https://www.privacyshield.gov/article?id=EU-US-Privacy-Shield-Programm.html> [10.05.2024].

[17] Thus expressly *Glocker F.*, EU-US Data Privacy Framework: Beschluss der EU-Kommission <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/eu-us-data-privacy-framework-beschluss-der-eu-kommission.html> [10.05.2024].

[18] The website can be found at <https://www.dataprivacyframework.gov/s.html> [10.05.2024].

[19] Decision (EU) 2023/4745 of the European Commission of 10 July 2023.

[20] On this in detail *Glocker F.*, EU-US Data Privacy Framework: Beschluss der EU-Kommission <https://www.cmshs-bloggt.de/datenschutzrecht/eu-us-data-privacy-framework-beschluss-der-eu-kommission.html> [10.05.2024].

საზედამხედველო ორგანოებს, დაუშვან მონაცემთა გადაცემა თვითსერტიფიცირებულ ამერიკულ კომპანიებზე.

ასევე ეფექტურად გამარტივებულია გადაცემა არათვითსერტიფიცირებულ ამერიკულ კომპანიებზე. მონაცემთა დამუშავებისთვის პასუხისმგებელმა პირებმა უნდა გააგრძელონ ხელშეკრულების სტანდარტული პირობების შეთანხმება არათვითსერტიფიცირებულ კომპანიებთან. ასეთ შემთხვევებში, მონაცემთა დაცვის ეროვნული საზედამხედველო ორგანოები ფაქტობრივად ვალდებულნი იქნებიან, შეამოწმონ მესამე ქვეყნის კანონმდებლობის შესაბამისობა მონაცემთა დაცვის ევროპულ სტანდარტებთან (ე.წ. გადაცემის ზემოქმედების შეფასება). იმის ნაცვლად, რომ განახორციელონ შეფასება, მხარეებს შეუძლიათ დაეყრდნონ გადაწყვეტილებას, არსებულ შეფასებას.[21]

არსებობს ეჭვი, „ტრანსატლანტიკური მონაცემთა კონფიდენციალურობის ჩარჩო“ შეთანხმება და ევროკომისიის შესაბამისობის გადაწყვეტილება რამდენად აკმაყოფილებს ევროკავშირის მართლმსაჯულების სასამართლოს მოთხოვნებს:

დამოუკიდებელი, კვაზი-სასამართლო ორგანოს შექმნა, რომელიც განიხილავს საჩივრებს მართლაც ეფექტიანი გამოსავალია და შესაძლოა აკმაყოფილებდეს სასამართლოს მოთხოვნებს სასამართლო დაცვის შესახებ. თუმცა, გაურკვეველია, დააკმაყოფილებს თუ არა აშშ-ს პრეზიდენტის აღმასრულებელი ბრძანების ფართო პირობები, რომელიც არეგულირებს აშშ-ს უსაფრთხოების სააგენტოების ფართო თვალთვალს, სასამართლოს მოთხოვნას მკაფიო და ზუსტი წესების შესახებ ასეთი ზომების მოცულობისა და გამოყენების შესახებ. გარდა ამისა, გამოქვეყნებული დოკუმენტები არ განმარტავს, თუ როგორ შემოიფარგლება აშშ-ს სააგენტოების თვალთვალი მხოლოდ იმით, რაც არის „აბსოლუტურად აუცილებელი“, როგორც ამას მოითხოვს “CJEU”.

„Trans-Atlantic Data Privacy Shield Framework“- შეთანხმების ბედი კიდევ ერთხელ შეიძლება გადაწყვიტოს “CJEU”-მ. სამოქალაქო უფლებების დამცველმა ორგანიზაციებმა, როგორიცაა “NOYB” [22] - ციფრული უფლებების ევროპული ცენტრი, რომელსაც ხელმძღვანელობს მაქსიმილიან შრემსი, უკვე განაცხადეს თავიანთი პოზიცია ევროკომისიის ახალი შესაბამისობის გადაწყვეტილების წინააღმდეგ. მსგავსი ინივიატივა გამოთქვა ფრანგმა ევროპარლამენტარმა ლატომბემ. თუმცა, ნაკლებად სავარაუდოა, რომ “CJEU” ამ საკითხზე მალე იმსჯელებს.[23]

შენიშვნა: პერსონალური მონაცემების სხვა მესამე ქვეყნებში გადაცემისთვის, რომელთა შესახებაც არ არსებობს ევროკომისიის შესაბამისობის გადაწყვეტილება, მართლმსაჯულების სასამართლოს 2020 წლის 16 ივლისის გადაწყვეტილება რჩება ძალაში.[24]

---

[21] *Glocker F.*, EU-US Data Privacy Framework: Beschluss der EU-Kommission <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/eu-us-data-privacy-framework-beschluss-dereu-kommission.html> [10.05.2024].

[22] „None Of Your Business“.

[23] See *Bernsdorff N.*, "EU-US Data Privacy Shield Framework" und der EuGH, Zeitschrift für den europäischen Datenschutz (ZED) 2023, 210, 213.

[24] *Bernsdorff N.*, "EU-US Data Privacy Shield Framework" und der EuGH, Zeitschrift für den europäischen Datenschutz (ZED) 2023, 210,214; *Glocker F.*, Politische Lösung für Datentransfers in die USA zeichnet sich ab <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/trans-atlantic-data-privacy-shield-framework.html> [10.05.2024]; also *Glocker F.*, EU-US Data Privacy Framework: Beschluss der EU-Kommission <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/eu-us-data-privacy-framework-beschluss-der-eu-kommission.html> [10.05.2024].

ბიბლიოგრაფია:

1. Charter of Fundamental Rights of the European Union, OJ 2010 L 83, 389.
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, OJ 2016 L 119, 1.
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281, 31.
4. Decision 2000/520/EC of the European Commission of 26 July 2000.
5. Decision (EU) 2016/1250 of the European Commission of 12 July 2016.
6. Decision (EU) 2023/4745 of the European Commission of 10 July 2023.
7. *Albrecht J. Ph.*, *Jotzo Fl.*, Das neue Datenschutzrecht der Europäischen Union, Baden-Baden, 2017.
8. *Bernsdorff N.*, „EU-US Data Privacy Shield Framework“ und der EuGH, Zeitschrift für den europäischen Datenschutz (ZED) 2023, 210.
9. *Eichenhofer E.*, „e-Privacy“ im europäischen Grundrechtsschutz: Das „Schrems“-Urteil des EuGH, Europarecht (EuR) 2016, 76.
10. *Glocker F.*, Politische Lösung für Datentransfers in die USA zeichnet sich ab <www.cmshs-bloggt.de> [10.05.2024].
11. *Glocker F.*, EU-US Data Privacy Framework: Beschluss der EU-Kommission <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/eu-us-data-privacy-framework-beschluss-der-eu-kommission.html> [10.05.2024].
12. *Kühling J.*, *Heberlein J.*, EuGH „reloaded“: „unsafe harbor“ USA vs. „Datenfestung“ EU, Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2016, 7.
13. *von Lewinski K.*, Privacy Shield – Notdeich nach dem Pearl Harbor für den transatlantischen Datenverkehr, Europarecht (EuR) 2016, 405.
14. *Rüpke G.*, *von Lewinski K.*, *Eckhardt J. (eds.)*, Datenschutzrecht – Grundlagen und europarechtliche Umgestaltung, Munich, 2018.
15. *Schantz P.*, *Wolff H. A.*, Das neue Datenschutzrecht, Berlin, 2017.
16. *Schreiber G.*, *Kohm W.*, Rechtssicherer Datenschutz unter dem EU-US Privacy Shield? – Der transatlantische Datenverkehr in der Unternehmenspraxis, Zeitschrift für Datenschutz (ZD) 2016, 255.
17. *Schwartmann R.*, Datentransfer in die Vereinigten Staaten ohne Rechtsgrundlage, Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2016, 864.
18. *Weichert Th.*, EU-US Privacy Shield – Ist der transatlantische Datenverkehr nun grundrechtskonform?, Zeitschrift für Datenschutz (ZD) 2016, 209.
19. *Wuermeling U.*, Handelshemmnis Datenschutz – Die Drittländerregelung der Europäischen Datenschutzrichtlinie, Berlin, 2000.
20. CJEU, Case C-362/14, *Maximillian Schrems/Data Protection Commissioner, Digital Rights Ireland Ltd.* („Schrems I“; 2015).
21. CJEU, Case C-311/18, *Data Protection Commissioner/Facebook Ireland Ltd., Maximillian Schrems* („Schrems II“; 2020).