ЕТИКА, ПРАВО И ТЕХНОЛОГИИ В КОНТЕКСТА НА ЗАЩИТАТА НА ЛИЧНАТА НЕПРИКОСНОВЕНОСТ И ЛИЧНИТЕ ДАННИ В ЕС
(Възможности за международно предаване на данни извън ЕС)

Доц. д-р Деница Топчийска, НБУ

ETHICS, RIGHTS AND TECHNOLOGIES IN THE CONTEXT OF PERSONAL DATA PROTECTION IN THE EU
(Possibilities for international data transfers outside the EU)

Associate Prof. Denitza Toptchiyska, PhD

Abstract: *Complex technology architecture and the Internet lead to inability to protect effectively the legal rights across the EU without a wider consensus on their content and significance. In this view, Regulation (EU) 2016/679 provides for a set of legal instruments designed to ensure the transfer of data from the EU to third countries and international organizations while maintaining a high level of protection. The publication analyzes the envisaged legal mechanisms for data transfer, focusing on the new aspects of legal regulation.*
Keywords: *data protection, international data transfers, EU General Data Protection Regulation (GDPR), certification, codes of conduct, standard contractual rules.*

Развитието на информационните и комуникационните технологии в последните години и възможностите, които те предоставиха на публичния и частния сектор за обработване и международен пренос на големи цифрови комуникационни потоци в реално време, стана предпоставка за значителни промени в икономическите и социалните модели. Технологичните иновации наложиха преосмислянето в нов контекст на правото за защитата на личната неприкосновеност и разработването на модели за защита на личните данни, чиято цел е, от една страна, да се гарантират основните права на лицата във връзка с обработването на техните данни и, от друга страна, да се осигури свободното движение на лични данни, като необходимост за развитието на глобалната цифрова икономика.[1]

Като резултат от продължителна реформа през 2016 г. Европейският съюз (ЕС) прие Регламент (ЕС) 2016/679 относно защитата на физическите лица във връзка с обработването на лични данни и свободното движение на такива данни (Общ регламент за защита на данните).[2] С него се отмени действащата в тази област Директива 95/46/ЕО[3], чиято оценка показа проблеми по отношение на нейната ефективност, свързани с разликите при въвеждането и прилагането ѝ в националните законодателства на държавите членки на ЕС.[4] Новият регламент предвижда единни правила, които ще бъдат директно приложими във всички държави членки на Съюза от 25 май 2018 г. Неговата

[1] Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите, Стратегия за цифров единен пазар за Европа, COM(2015) 192 final, 6.5.2015, стр. 3 и стр. 15

[2]Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), ОВ L 119, 4.5.2016г., стр. 1—88

[3]Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни, ОВ L 281, 23.11.1995г., стр. 31—50. Директивата ще бъде отменена, считано от 25 май 2018 г., когато влиза в сила Регламент (ЕС) 2016/679

[4]Robinson N., Graux H., Botterman M., andValeri L. (2009), ReviewoftheEuropean Data ProtectionDirectiveonlineat http://www.hideproject.org/downloads/references/review_of_eu_dp_directive.pdf (accessed 25.04.2014)

цел е да се гарантира последователно и високо ниво на защита на данните на физическите лица в рамките на Съюза, като се подпомогне развитието на Единния цифров пазар.[5]

Сложната технологична архитектура и интернет пространството са свързани с невъзможност юридическите права да бъдат ефективно защитени на територията на ЕС, без да има наличие на консенсус в по-широк мащаб за тяхното съдържание и значимост. В повечето анализи например облачните услуги са разделени на три нива: предоставяне на инфраструктура, софтуер и платформа, които често включват много компании, установени в различни юрисдикции по света.[6] С оглед на това Регламент (ЕС) 2016/679 предвижда комплекс от правни инструменти, чиято цел е да се гарантира възможността за трансфер на данни от ЕС към трети държави и международни организации при запазване на висока степен на тяхната защита. Настоящата публикация анализира предвидените правни механизми за пренос на данни, като акцентира върху новите аспекти в правното регулиране.

Защитата на личните данни като концепция в правното регулиране започва да се развива през 60-те години на 20-и век в отговор на предизвикателствата, които информационните и комуникационните технологии поставят по отношение защитата на правото на лична неприкосновеност в глобален контекст. Правни инструменти в тази област се разработват от ООН[7], Съвета на Европа[8], Европейския съюз[9] и Организацията за азиатско-тихоокеанско икономическо сътрудничество.[10] Значение придобиват Насоките за защита на личните данни, приети от Организацията за икономическо сътрудничество и развитие,[11] както и някои регионални инициативи.[12] Независимо че във всички правни рамки е възприет общ модел за защита на личните данни, базиран на сходни понятия и принципи, той придобива различна конкретизация по отношение на предоставената степен на защита на правото на лична неприкосновеност и баланса, който се поставя с оглед на конкуриращите се с него интереси, като например защитата на сигурността, свободата на информация и защитата на интересите, свързани с развитието на бизнес средата и т. н. За България темата за защитата на личните данни става актуална едва след промените от 1989 г. Причините за късното й поставяне се дължат и на това, че в периода от 1944 г. до 1989 г. всяка сфера на професионална и обществена дейност е подчинена на държавата.[13]

Първата обща правна рамка за защита на личните данни в ЕС е въведена през 1995 г. с приемането на Директива 95/46/ЕО. Тя се основава на модела, възприет от Съвета на Европа в Конвенция 108 за защита на лицата при автоматизираната обработка на лични данни от 1981 г.[14] С Договора за функциониране на ЕС, подписан през 2007 г., се

---

[5]Член 1 във връзка съображение (7) от Регламент (ЕС) 2016/679

[6]Gasser U. (2014), CloudInnovationandtheLaw: Issues, Approaches, andInterplay, BerkmanCenter, onlineatSeries: http://cyber.law.harvard.edu/research/cloudcomputing (accessed 25.04.2014)

[7] Guidelines for the Regulation of Computerized Personal Data Files adopted by General Assembly resolution 45/95 on 15 December 1989 (Document E/CN.4/1990/72).

[8]Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981

[9]Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 година за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни, ОВ L 281, 23.11.1995г., стр. 31—50

[10] APEC Privacy Framework (2015), https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)

[11]OECD'sGuidelinesontheProtectionofPrivacyandTrans-BorderFlowsofPersonal Data (OECD Guidelines), http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[12]United Nations, UNCTAD, Data protection regulations and international data flows: Implications for trade and development, 2016, p. 35-36

[13]Михайлова, Е., Тоталитарната държава и право в България 1944-1989г., НБУ, 2016, с.12

[14] Council of Europe, Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28/01/1981

предвиди приемането на правила за защитата на личните данни, които да се прилагат в всички области в рамките на компетентността на Съюза.[15] Като потвърждение за неговата значимост в политиката на ЕС правото на защита на личните беше защитено като самостоятелно право, отделно от правото на лична неприкосновеност, в Хартата на основните права в ЕС от 2007 г. То се свърза с третата генерация модерни права и се конкретизира в три насоки: като комплекс от принципи за обработване на личните данни, права на субектите на лични данни и изискване за наличие на независим надзорен орган, който да осъществява необходимия контрол.[16] Следва да се отбележи, че в своята практика Съдът на ЕС също така затвърди позицията на Съюза за необходимостта от гарантиране на висока степен на защита на лична неприкосновеност и в частност на личните данни в контекста на информационното общество.[17] По този начин се гарантира в пълнота един от принципите на правовата държава, изразяващ се в защита на основните човешки и граждански свободи.[18]

Приетият от ЕС през 2016 г. Общ регламент за защита на данните утвърждава европейския модел за защита на личните данни, чиято цел е да гарантира висока степен на защита на правото на лична неприкосновеност и правото на човешко достойнство, като същевременно не се ограничават възможностите, предлагани от глобалното информационно общество. С него се актуализират разпоредбите на Директива 95/46/ЕО за защита на личните данни на ЕС и се възприемат решения, които са в съответствие с практиката на Съда на ЕС в тази област. Същевременно с приемането на Регламент (ЕС) 2016/679 възникват нови понятия и права, като правото да бъдеш забравен[19], правото на преносимост на данните[20], защита на данните на етапа на проектирането и по подразбиране[21], изискване за уведомления при нарушаване на сигурността на данните или извършване на оценка на въздействието, свързана със защитата на личните данни.[22] Тези допълнения имат за цел да предоставят по-голям контрол на физическите лица върху личните им данни и да засилят доверието на потребителите в цифровата икономика. С новия Регламент (ЕС) 2016/679 се правят и значителни промени по отношение възможностите за трансфер на данни от ЕС към трети държави и международни организации, които са предмет на анализ по-надолу.

1. Материален обхват на Регламент (ЕС) 2016/679

Правилата за предаване на данни към трети държави или международни организации, предвидени в Регламент (ЕС) 2016/679, се прилагат единствено в рамките на материалния обхват на регламента. В него попада всяко обработване на лични данни в частния или публичния сектор, което е в рамките на приложното поле на правото на ЕС. От обхвата на регламента са изключени изрично случаите на обработване на данни от физически лица в хода на техните лични или домашни занимания. В своето решение от 11 декември 2014 г. по делото C 212/13 Съдът на ЕС тълкува това изключение, което беше предвидено също така в Директива 95/46/ЕО, като напомня, че в съответствие с установената практика, защитата на правото на лична неприкосновеност, гарантирано в член 7 от Хартата на основните права в ЕС, изисква дерогациите или изключенията във връзка със защитата на личните данни да бъдат прилагани само дотолкова, доколкото е

[15]Чл. 16 от Договора за функционирането на ЕС, Консолидиран текст на Договора за функционирането на Европейския съюз, ОВ C 326, 26.10.2012, p. 47–390
[16]Чл. 8 от Хартата на основните права на Европейския съюз, ОВ C 326, 26.10.2012г., стр. 391—407
[17]напр.CJEU, C-101/01, BodilLindqvist, 6 November 2003; C-131/12, GoogleSpain, S.L., GoogleInc. v. AgenciaEspañoladeProteccióndeDatos, MarioCostejaGonzález, 13 May 2014;
[18]Михайлова, Е., Парламентаризъм и правова държава в България, НБУ, 2012, с.25
[19]Чл. 17 от Регламент (ЕС) 2016/679
[20]Чл. 20 от Регламент (ЕС) 2016/679
[21]Чл. 25 от Регламент (ЕС) 2016/679
[22]Чл. 35 от Регламент (ЕС) 2016/679

строго необходимо.[23] Освен това те трябва да бъдат тълкувани ограничително. Съдът подчертава, че това изключение се прилага само в случаите, когато обработването е за „изцяло“ лични или домашни занимания и следователно всички дейности, които са насочени извън личната сфера на физическите лица и не са „изцяло“ лични или домашни дейности, не попадат в неговия обхват.[24]

Регламент (ЕС) 2016/679 не се прилага по отношение на обработването на лични данни в рамките на общата външна политика и политиката на сигурност на ЕС (дял 5, глава 2 от Договора за Европейския съюз), както и в случаите на обработване на данни от компетентните органи в рамките на наказателното преследване. В последната област се прилага Директива (ЕС) 2016/680 за полицейското сътрудничество във връзка с обработването на данни за целите на наказателното преследване и изпълнението на наказанията. Директивата влезе в сила на 5 май 2016 г., а държавите членки на ЕС трябва да я транспонират в националното си право до 6 май 2018 г.[25].

2. Териториален обхват на Регламент (ЕС) 2016/679

По отношение прилагането на възможностите за пренос на данни към трети държави или международни организации е важно изясняването също така на териториалния обхват на Регламент (ЕС) 2016/679. Регламентът се прилага на територията на ЕС и в рамките на Европейското икономическо пространство (ЕИП), което обхваща Исландия, Норвегия и Лихтенщайн. Както в Директива 95/46/ЕО, така и в Регламент (ЕС) 2016/679 се възприема общия принцип, че движението на данни на територията на ЕС и ЕИП е свободно. Регламент (ЕС) 2016/679 предвижда, че свободното движение на лични данни в рамките на Съюза не се ограничава, нито се забранява по причини, свързани със защитата на физическите лица във връзка с обработването на лични данни.[26] Също така следва да се отбележи, че в новия регламент беше въведена дефиниция на понятието „трансгранично обработване“ („cross-border processing“) относно случаи на обработване на данни в ЕС, които засягат няколко държави-членки.[27] Тези случаи следва да се разграничават от международното предаване на данни към трети държави, а именно към държави извън ЕС и ЕИП или международни организации, които са предмет на анализ в публикацията. Същевременно Конвенция 108 на Съвета на Европа използва термина трансгранични потоци от данни ("transborded data flows") по отношение на всяко предаване на данни през граница, което следва да се има предвид при прилагането на конвенцията.[28]

По отношение на териториалния обхват в Регламент (ЕС) 2016/679 са въведени нови правила, чиято цел е да се постигне яснота в сравнение с Директива 95/46/ЕО, както и да се защитят в по-голяма степен интересите на лицата, които се намират на територията на ЕС. Необходимо е да се подчертае, че защитата на Регламента е насочена

---

[23]JUDGMENT OF ECJ of 11 December 2014, Referencefor a preliminaryrulinginCase C-212/13,František Ryneš v Úřadproochranuosobníchúdajů, par. 28

[24]По цитираното дело Съдът на ЕС се произнася, че "използването на система за видеонаблюдение, извършваща видеозаснемане на хора, съхранявано върху устройство за дълготрайно запаметяване, а именно твърд диск, която е инсталирана от физическо лице в семейната му къща за защита на собствеността, здравето и живота на собствениците на къщата, като системата покрива и обществени места, не представлява обработване на лични данни при извършване на изцяло лични или домашни занимания по смисъла на тази разпоредба." - JudgmentofECJof 11 December 2014, ReferenceforapreliminaryrulinginCaseC-212/13, FrantišekRyneš vÚřadproochranuosobníchúdajů, par. 35

[25]Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета (ОВ L 119, 4.5.2016 г., стр. 89).

[26]Член 1, параграф 3 от Регламент (ЕС) 2016/679

[27]Член 4, параграф 23 от Регламент (ЕС) 2016/679

[28]България е ратифицирала Конвенция 108 на Съвета на Европа през 2002 г. и тя е в сила за България от 1 януари 2003 г.

към всички физически лица, които се намират на територията на ЕС, независимо от тяхното гражданство.[29]За разлика от Директива 95/46/ЕО, която обвързваше прилагането й единствено с мястото на установяване на администратора на обработването, Регламент (ЕС) 2016/679 предвижда, че неговите правила ще са приложими по отношение както на администратори, така и на обработващи лични данни, които имат място на установяване на територията на ЕС, когато обработването е в контекста на осъществяваните от тях дейности, независимо дали обработването се осъществява на територията на ЕС или извън него. Регламентът ще сеприлага също така и по отношение на администратори и обработващи лични данни, които не са установени в ЕС, когато дейностите по обработване на данни, които осъществяват, са свързани с предлагането на стоки или услуги на субекти на данни, които се намират в Съюза. Разпоредбите на регламента ще са приложими независимо дали предлаганите услуги са безплатни или срещу заплащане. Когато обработването на данни е свързано с наблюдение на поведението на лица, което се проявява в рамките на ЕС, също трябва да се прилага Регламент (ЕС) 2016/679 дори и в случаите, когато администраторът и обработващият личните данни не са установени в ЕС. Целта на тези разпоредби е да се създадат условия за равнопоставеност между европейските и чуждестранните дружества, тъй като дружествата, установени извън ЕС, ще прилагат същите правила като европейските дружества, ако предлагат стоки и услуги или наблюдават поведението на физически лица в ЕС. Също така следва да се отбележи по-детайлизираната уредба в сравнение с Директива 95/46/ЕО, която е предпоставка за повече яснота и правна сигурност при прилагането на регламента, както и избягването на законодателни празноти.

3. Кога е налице предаване на лични данни към трети държави или международни организации

Предаване на данни към трети държави или международни организации е налице в случаите, когато лични данни се обработват или са предназначени за обработване след предаването им към трета държава или международна организация.[30]На практика с Регламент (ЕС) 2016/679 се запазва дефиницията, предвидена в Директива 95/46/ЕС. В своето решение от 2003 г. по делото *Bodil Lindqvist* Съдът на ЕС се произнася, че няма трансфер на данни към трети държави по смисъла на Директива 95/46/ЕС, когато лице в рамките на държава членка на ЕС поставя лични данни на Интернет страница, която се съхранява от хостинг компания, намираща се на територията на ЕС, независимо че тези данни стават достъпни за всеки, който се свърже с Интернет, включително и лица от трети държави.[31] Принципът, че обикновеното публикуване на лични данни в интернет не се приема за пренос на данни към трети държави, се прилага и по отношение на публичните регистри[32] и масовите онлайн медии, като електронни вестници и телевизия. Единствено комуникацията, която е насочена към конкретен субект или субекти, може да бъде включена в понятието за предаване на данни към трети държави или международни организации.[33]

4. Правни възможности за предаване на данни към трети държави или международни организации

Общият принцип, предвиден в Регламент (ЕС) 2016/679, е, че трансферът на лични данни към трети държави или международни организации е допустим само ако

[29]Член 3, параграф 2 от Регламент (ЕС) 2016/679

[30]Член 44 от Регламент (ЕС) 2016/679

[31]CJEU, C-101/01, Bodil Lindqvist, 6 November 2003, paras.68, 69 and 71

[32]Напр. публичните регистри за държавни помощи: Валериева, Г. Правомощия на Европейската Комисия при отпускането на държавна помощ. De Jure.2012, №2, 49-58 и Симеонова, Г. Нови процедурни правила за държавната помощ като публично държавно вземане. Норма.2016, бр. 2 ,49-68 и публичните регистри по европейските фондове: Михайлова, С. Финансови правни отношения в системата на публичните средства от европейските структурни и инвестиционни фондове“, С., Сиела, 2017

[33]European Union Agency for Fundamental Rights, 2014 and Council of Europe, 2014, Handbook on European Data Protection Law, p. 131

администраторът и обработващият на личните данни спазват условията на Регламент (ЕС) 2016/679, включително особените изисквания по отношение на този тип предаване на данни, които са предвидени в него.[34] В своето Съобщение „Обмен и защита на личните данни в един глобализиран свят“ Европейската комисия подчертава важното значение, което има международното предаване на данни за развитието на глобалната цифрова икономика.[35] Същевременно се насочва вниманието към необходимостта то да се осъществява при спазването на стандартите за защита на личната неприкосновеност, гарантирани в модела на ЕС за защита на личните данни. С оглед на това в Регламент (ЕС) 2016/679 са предвидени различни правни механизми, чрез които в рамките на търговския сектор да се предостави възможност за трансфер на данни на лица от ЕС към трети държави. Целта на новия Регламент е да опрости правилата за международен пренос на данни в сравнение с Директива 95/46/ЕС, както и да въведе нови инструменти за предаване на данни, които да осигурят ефективни възможности, адекватни на конкретните обстоятелства.[36]

Предвидените в Регламент (ЕС) 2016/679 правни възможности за трансфер на данни към трети държави и международни организации могат да бъдат разделени в три основни групи. Първата група включва общото разрешение за трансфер на данни към трети държави или международни организации, които предоставят „адекватно ниво на защита на данните“. Втората група от възможности обхваща комплекс от алтернативни механизми, въз основа на които могат да бъдат пренесени данни, въпреки липсата на адекватно ниво на защита на данните в съответната държава или международна организация. Третата група от възможности обхваща комплекс от дерогации, които могат да се приложат при липса на решение на Европейската комисия (ЕК) относно наличието на адекватното ниво на защита на данните или подходящи гаранции в рамките на предвидените в Регламент (ЕС) 2016/679 алтернативни механизми.

4.1. Решение на ЕК за наличието на адекватно ниво на защита на данните

Регламент (ЕС) 2016/679 предвижда общо разрешение за предаване на данни към трети държави или международни организации, относно които е признато наличието на адекватно ниво на защита.[37] Решението за признаване на адекватно ниво на защита се приема от ЕК след становище от Европейския комитет по защита на данните (ЕКЗД).[38] То се прилага на територията на всички държави членки на ЕС и ЕИП, като позволява свободния поток на лични данни от ЕС/ЕИП към съответната трета държава или международна организация, без да е необходимо износителят на данни да получи разрешение от компетентния надзорен орган.

В Регламент (ЕС) 2016/679 е изрично предвидена възможността решението на ЕК за адекватност да бъде не само по отношение на дадена трета държава или международна организация, но и по отношение на отделна територия (географска област), конкретен сектор или промишлен отрасъл в тазидържава. Тази възможност е предпоставка за по-гъвкав подход от страна на ЕК, като се признава т. нар.„частично“ адекватно ниво на защита.

Концепцията за „адекватно ниво на защита“, която съществува и в отменената Директива 95/46, е изяснена в практиката на Съда на ЕС и по-конкретно в решението по

[34]Член 44 от Регламент (ЕС) 2016/679

[35]Съобщение на Комисията до Европейския парламент и Съвета "Обмен и защита на личните данни в един глобализиран свят", Брюксел, 10.1.2017 г. COM(2017) 7 final, стр. 16

[36] Следва да се отбележи , че личните данни могат да се класифицират като информация от частен интерес. За класифицирането на видовете информация виж повече в Николова, Р. Административноправна същност на информацията. София, Дружество за Европейско право, 2016 г. с. 61 – 65.

[37]Член 45, параграф 1 от Регламент (ЕС) 2016/679

[38]Чл. 70, параграф 1, буква т) от Регламент (ЕС) 2016/679

делото *MaximillianSchrems*.[39] В него Съдът приема, че, за да бъде адекватно нивото на защита в третата държава, то трябва да бъде еквивалентно „по своето същество“ на това, което е гарантирано в ЕС.[40] Това означава според решението на Съда на ЕС, че от съответната трета държава се изисква ефективно да гарантира, по силата на вътрешното си законодателство или на международните си споразумения, степен на защита на основните права и свободи, която по същество е равностойна на гарантираната в ЕС по силата на Директива 95/46, разглеждана във връзка с Хартата за правата на човека на ЕС. Независимо че е възможно средствата, които използва третата държава да бъдат различни от прилаганите вътре в Съюза, необходимо е те на практика да осигуряват ефективна защита, която по същество е равностойна на гарантираната в ЕС. Следователно при преценката трябва да се вземат предвид както съществуващите материалноправни разпоредби, така и процесуалните възможности за защита.

На основата на практиката на ЕК по Директива 95/46/ЕО и на Съда на ЕС, в Регламент (ЕС) 2016/679 са предвидени конкретните критерии, които трябва да бъдат взети предвид с оглед оценката на нивото на защита в съответната трета държава или международна организация.[41] Те включват преценка относно наличието на върховенство на правото, защита на правата на човека и основните свободи. Трябва да се анализира също така вътрешното законодателство (общо и секторно) и съдебната практика, включително в областта на обществената сигурност, отбраната, националната сигурност, наказателното право и възможността за достъп на публичните институции до лични данни. При преценката на нивото на защита ЕК трябва да вземе предвид и международните споразумения, към които се е присъединила съответната държава, като особено внимание се отделя на Конвенция 108 на Съвета на Европа за защита на лицата при автоматизираната обработка на лични данни.[42]

В процеса на анализ ЕК трябва да направи преценка кой подход би бил по-ефективен - цялостно или частично признаване на адекватност, като се вземе предвид естеството и степента на развитие на правния режим на неприкосновеността на личния живот (отделен закон, множество закони или секторни закони и т. н.), конституционната рамка на третата държава или конкретните обстоятелството в даден сектор на икономиката.[43] В съответствие с изискванията на Регламент (ЕС) 2016/679 при приемането на решението за адекватност на защитата ЕК трябва задължително да предвиди механизъм за периодичен преглед на нивото на защита в съответната държава, при който се отчитат всички имащи отношение промени. При необходимост ЕК може да отменя, изменя или спира прилагането на решението, като започва консултации с третата държава или международната организация, за да коригира положението. Комисията публикува в Официален вестник на Европейския съюз и на своя уебсайт списък на трети държави, територии и конкретни сектори в трета държава и международни организации, за които е решила, че осигуряват или че вече не осигуряват адекватно ниво на защита.

Подробното дефиниране на критериите за оценка на адекватността в Регламент (ЕС) 2016/679 има за цел да подпомогне не само институциите на ЕС, но също така и трети държави и международни организации, които биха искали да получат признание за еквивалента защита. В работната програма на Европейската комисия, свързана с прилагането Регламент (ЕС) 2016/679 се предвижда Работната група по член 29 от

[39]Case C-362/14, MaximillianSchrems v Data ProtectionCommissioner, 6 October 2015
[40]Case C-362/14, MaximillianSchrems v Data ProtectionCommissioner, 6 October 2015, par. 73, 74
[41]Член 45, параграф 2, букви а), б) и в) от Регламент (ЕС) 2016/679
[42]Съображение 105 от Регламент (ЕС) 2016/679
[43]Съобщение на Комисията до Европейския парламент и Съвета "Обмен и защита на личните данни в един глобализиран свят", Брюксел, 10.1.2017 г. COM(2017) 7 final, стр. 10

Директива 95/46/ЕО, която ще се трансформира в ЕКЗД, да приеме актуализирани насоки по отношение на адекватността (Референтен документ относно адекватността).[44]

Решенията на ЕК относно адекватността, приети в съответствие с член 25, параграф 6 от Директива 95/46/ЕО, остават в сила след приемането на Регламент (ЕС) 2016/679, като трансферът на данни към тези държави е свободен, докато съответните решения не бъдат изменени или отменени.[45]Към момента ЕК е приела решения за наличието на адекватна защита на личните данни в Андора, Аржентина, Канада, Фарьорските острови, Гърнзи, Израел, остров Ман, Джърси, Нова Зеландия, Швейцария, Уругвай и САЩ. Решенията за адекватност относно Канада и Съединените щати са констатации за частично адекватно ниво на защита. Решението за адекватност в Канада се прилага единствено по отношение на търговски организации, чиято дейност, свързана с обработване на данни, се регламентира от националния Закон за защита на личните данни и електронните документи.[46]

Първото решение на ЕК от 2000 г. за признаване на адекватно ниво на защита на данните в отношенията между ЕС и САЩ е известно като „Safe Harbour Privacy Principles“.[47] То е насочено към американски бизнес компании, които доброволно декларират своят ангажимент пред Търговския департамент на САЩ да прилагат предвидените в споразумението принципи. С решението на Съда на ЕС по делото *MaximillianSchrems* Решението на ЕК за приемането на принципите на Safe Harbour е обявено за невалидно.[48] Основният аргумент на Съда на ЕС е, че с решението се ограничават правата на надзорните органи да вземат мерки с цел гарантиране на спазването принципите на правото на ЕС за защита на личните данни при международния пренос на данни. Съдът на ЕС приема, че с решенията на ЕК за признаването на адекватност на нивото на защита на данните не може да се намалят или да се елиминират правомощията на Националните надзорни органи в съответствие с Хартата на ЕС за основните права и Директива 95/46/ЕО.

През 2016 г. е прието ново решение на ЕК за признаване на адекватност на защитата в САЩ, известно като „Щит за личните данни“ (PrivacyShield)[49], за приемането на което са взети предвид заключенията на Съда на ЕС по делото *MaximillianSchrems*. В него се предвижда, че присъединилите се дружества ще прилагат предвидените в споразумението стандарти, като контролът ще се осъществява в съответствие с правото на САЩ. При приемането на решението си за адекватност ЕК е взела предвид писмените изявления на правителството на САЩ по отношение на достъпа до лични данни за целите

[44]Съобщение на Комисията до Европейския парламент и до Съвета, По-силна защита, нови възможности — насоки на Комисията относно прякото прилагане, считано от 25 май 2018 г., на Общия регламент относно защитата на данните/FMT, COM(2018) 43 final, Брюксел, 24.1.2018

[45]Чл. 45, пар. 9 от Регламент (ЕС) 2016/679

[46] European Commission (2002), Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, OJ 2002 L 2.

[47] European Commission (2000), Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ 2000 L 215.

[48]Case C-362/14, MaximillianSchrems v Data ProtectionCommissioner, 6 October 2015 (§ 106);

[49]CommissionImplementingDecision (EU) 2016/1250 of 12 July 2016 pursuanttoDirective 95/46/ECoftheEuropeanParliamentandoftheCouncilontheadequacyoftheprotectionprovidedbytheEU-U.S. PrivacyShield (notifiedunderdocumentC(2016) 4176) (TextwithEEArelevance), OJL 207, 1.8.2016, p. 1–112/ РЕШЕНИЕ ЗА ИЗПЪЛНЕНИЕ (ЕС) 2016/1250 НА КОМИСИЯТА от 12 юли 2016 година съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета относно адекватността на защитата, осигурявана от Щита за личните данни в отношенията между ЕС и САЩ (EU-U.S. PrivacyShield) (нотифицирано под номер С(2016) 4176) (текст от значение за ЕИП)

на националната сигурност, включително назначаването на омбудсман, който да разглежда жалби на граждани от ЕС.[50]

Към момента ЕК води преговори за установяване на адекватно ниво на защита с ключови търговски партньори в Латинска Америка и Азия, като са започнали преговорите с Индия, Япония и Китай. Преценката за започване на преговори със следващи държави е свързана с тяхната роля като търговски партньор на ЕС и обема на трансфер на данните от ЕС към съответните държави.

4.2. Алтернативни правни механизми за международен пренос на данни

При липса на решение на ЕК за установяване на адекватността на защитата в трета държава или международна организация, администраторите или обработващите данниот ЕС/ЕИП могат да предават лични данни към нея при наличие на подходящи гаранции за спазване на изискванията на Регламент (ЕС) 2016/679, включително приложими права на субектите на данни и ефективни правни средства за защита. Тези гаранции могат да бъдат осигурени чрез предвидените в регламента алтернативни правни инструменти, които дават възможност да се вземат предвид конкретните нужди или условия на специфичните отрасли, бизнес модели и/или групи администратори /обработващи данни. Такива алтернативни правни инструменти за организациите от частния и публични сектор са стандартните договорни клаузи, задължителните фирмени правила, кодексите за поведение и механизмите за сертифициране. Следва да се отбележи, че извън тези възможности публичните органи могат да предвидят необходимите гаранции и в рамките на друг правен инструмент, който има задължителен характер и изпълнителна сила.[51]

4.2.1. Стандартни договорни клаузи

Стандартните договорни клаузи са правен механизъм, който е бил предвиден в Директива 95/46/ЕО.[52] В съответствие с директивата компетентен орган да одобри стандартните договорни клаузи е ЕК. След одобряването им те имат задължителен характер по отношение на държавите членки, а националните надзорни органи трябва да признаят тяхното действие. Критерият, за да бъдат одобрени клаузите, е да съдържат мерки, които осигуряват достатъчни гаранции за защитата на личния живот и основните права и свободи на лицата, както и да предвиждат ефективни възможности за упражняването на техните права, свързани със защитата на личните данни. Към момента ЕК е одобрила два типа стандартни договорни клаузи: първо, между администратор на лични данни в ЕС/ЕИП и администратор на личните данни извън ЕС/ЕИП[53] и второ, между администратор на лични данни в ЕС/ЕИП и обработващ личните данни извън ЕС/ЕИП.[54] В стандартните договорни клаузи се съдържа правно задължителна разпоредба, че както износителят, така и вносителят на данните се задължат да

[50]Съобщение на Комисията до Европейския парламент и Съвета "Обмен и защита на личните данни в един глобализиран свят", Брюксел, 10.1.2017 г. COM(2017) 7 final, стр.8

[51]Член 46, параграф 2, буква а) от Регламент (ЕС) 2016/679

[52]Член 26, параграф 4 от Директива 95/46/ЕО

[53]РЕШЕНИЕ НА КОМИСИЯТА от 15 юни 2001 година относно общите договорни клаузи за трансфера на лични данни към трети страни съгласно Директива 95/46/ЕО (нотифицирано под номер С(2001) 1539) (текст от значение за ЕИП) (2001/497/ЕО); РЕШЕНИЕ НА КОМИСИЯТА от 27 декември 2004 година за изменение на Решение 2001/497/ЕО за въвеждане на алтернативен комплект общи договорни клаузи за прехвърляне на лични данни в трети страни (нотифицирано под номер С(2004) 5271)(текст от значение за ЕИП)(2004/915/ЕО)

[54]РЕШЕНИЕ НА КОМИСИЯТА от 5 февруари 2010 година относно стандартните договорни клаузи при предаването на лични данни към лицата, които ги обработват, установени в трети страни, съгласно Директива 95/46/ЕО на Европейския парламент и на Съвета (нотифицирано под номер С(2010) 593)(текст от значение за ЕИП)(2010/87/ЕС)

обработват данните в съответствие с основните принципи за защита на данните в ЕС и, че субектите на личните данни могат да упражнят правата си в рамките на договора, независимо че не са страна по него. Също така двете страни се съгласяват да бъдат под контрола на надзорен орган и на съдебна юрисдикция в ЕС.[55]

Съгласно Директива 95/46/ЕО стандартните договорни клаузи можеха да бъдат включени като част от по-голям договор. Също така наличието на одобрени клаузи не беше пречка страните да разработят adhoc клаузи за конкретен случай, които да гарантират еквивалентно ниво на защита, но за тяхното прилагане се изискваше специално одобрение от страна на компетентния надзорен орган.

В съответствие с Регламент (ЕС) 2016/679 стандартните договорни клаузи трябва да бъдат приети от ЕК или да бъдат приети от национален надзорен орган и одобрени от Комисията.[56]Регламент (ЕС) 2016/679 съдържа възможността договорни клаузи за защита на данните да бъдат разработени adhoc между износителя и получателя на данните в трета държава или международна организация, за конкретен случай, при условие че компетентния надзорен е дал разрешение за това.[57] Страни по договора могат да бъдат както администратори на данните, така и обработващи личните данни. Следователно клаузите могат да бъдат включени в договор между администратори/ обработващи лични данни, установени в ЕС/ЕИП, и администратори/ обработващи лични данни в държави извън ЕС/ЕИП.

Регламент (ЕС) 2016/679 предвижда, че решенията на ЕК за одобряване на стандартни договорни клаузи в съответствие с член 26, параграф 4 от Директива 95/46/ЕО остават в сила, докато не бъдат изменени, заменени или отменени от ЕК.Те могат да бъдат изменени, заменени или отменени, ако е необходимо от компетентния надзорен орган. В сила ще останат и разрешенията на надзорните органи за одобряване на договорни клаузи adhoc, докато не бъдат изменени, заменени или отменени от надзорния орган, който ги е издал.[58] Независимо от това Работната група по член 29 съветва те да бъдат съобразени с изискванията на Регламент (ЕС) 2016/679 преди влизането му в сила на 25 май 2018 г.

4.2.2. Задължителни фирмени правила

Задължителните фирмени правила са алтернативен правен механизъм за международен пренос на данни, който е насочен към частния сектор. В съответствие с Директива 95/46/ЕО те представляваха съвкупност от правила, приложими по отношение на мултинационална група от компании, намиращи се в ЕС и в трети държави, за които не е признато адекватност на нивото на защита с решение на ЕК. В задължителните фирмени правила се определя начина за осъществяване на международно предаване на данни в рамките на групата от компании. След като са одобрени по съответния ред, трансферът на данни към компаниите в рамките на групата, независимо къде се намират, става свободно. Работната група по член 29 от Директива 95/46/ЕО предвиди множество изисквания по отношение на съдържанието и структурата на задължителните фирмени правила.[59]

---

[55]European Union Agency for Fundamental Rights, 2014 and Council of Europe, 2014, Handbook on European Data Protection Law, p. 138

[56]Член 46, параграф 2, букви в) и г) от Регламент (ЕС) 2016/679

[57]Член 46, параграф 3 от Регламент (ЕС) 2016/679

[58]Член 46, параграф 5 от Регламент (ЕС) 2016/679

[59] Article 29 Working Party (2008), Working document setting up a framework for the structure of Binding Corporate Rules, WP 154, Brussels, 24 June 2008; and in Article 29 Working Party (2008), Working document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 153, Brussels, 24 June 2008.

Регламент (ЕС) 2016/679 разширява приложението на задължителните фирмени правила, като допуска те да се използват от група предприятия, които развиват съвместна стопанска дейност, без да е необходимо те да бъдат част от една и съща корпоративна група.[60] Задължителните правила се одобряват от компетентния надзорен орган в съответствие с механизма за съгласуваност, като техните задължителни реквизити са предвидени в Регламент (ЕС) 2016/679. Те трябва да имат правно задължителен характер и да са приложими спрямо всеки член на групата. Също така задължителните фирмени правила трябва изрично да осигуряват на субектите на данни правата, предвидени в Регламент (ЕС) 2016/679, както и да предвиждат, че администраторът или обработващият лични данни, установен на територията на държава членка, ще поеме отговорност за всяко нарушение на задължителните фирмени правила от друг член на съответната група, който не е установен в Съюза. В съответствие с изискванията на Регламент (ЕС) 2016/679 трябва да бъдат предвидени механизми за проверка на спазването на задължителните фирмени правила, както и механизъм за сътрудничество с надзорния орган, с който трябва да се осъществява непрекъснат обмен на информация.

За да се улесни използването на задължителните фирмени правила като инструмент за международни трансфери на данни, в контекста на подготовката за прилагането на Регламент (ЕС) 2016/679, Работната група по член 29 прие два нови документа - насоки, които се отнасят съответно до администраторите на лични данни и обработващите лични данни. Насоките за задължителните фирмени правила за обработващи лични данни се отнасят за случаите, когато изпращач на данните е обработващ лични данни, установени в ЕС, който не е член на групата и данните се обработват от членове на групата като обработващи организации. Насоките за задължителните фирмени правила за администратори на лични данни са насочени към изясняване на правилата за международен трансферна данни от администратор, установен в ЕС, до друг администратор или обработващ данните, които е извън ЕС и е в същата група.[61]

В съответствие с член 46, параграф 5 от Регламент (ЕС) 2016/679 съществуващите решенията на ЕК за одобряване на задължителни фирмени правила ще останат в сила, докато не бъдат изменени, заменени или отменени от ЕК.

4.2.3. Кодекси за поведение

Кодексите за поведение са механизъм, чиято цел е да се подпомогне прилагането на Регламент (ЕС) 2016/679, като се конкретизират неговите разпоредбите с оглед спецификите на отделните сектори (напр. брой заети и размер на предприятията). Инициатор за разработването на кодекси за поведение могат да бъдат сдружения или други структури, представляващи категории администратори или обработващи лични данни.[62] Надзорните органи и ЕКЗД трябва да насърчават разработването на кодекси за поведение.

Когато кодексът за поведение не засяга дейности по обработване на данни в различни държави членки, той се одобрява от компетентния надзорен орган. Същият надзорен орган трябва да регистрира и публикува кодекса за поведение. В случаите, в които кодексът за поведение има отношение към дейности по обработване в няколко държави членки, компетентният надзорен орган го предлага за съгласуване на ЕКЗД. Ако становището на ЕКЗД е положително, той го предоставя на ЕК. Комисията може чрез изпълнителен акт да реши дали одобреният кодекс за поведение е общовалиден в рамките на съюза, като осигурява публичност на документа. ЕКЗД от своя страна събира

[60]Член 47, параграф 2, буква а) от Регламент (ЕС) 2016/679

[61] Article 29 WP, Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules (updated) Adopted on 29 November 2017

[62]Член 40, параграф 2 от Регламент (ЕС) 2016/679

всички одобрени кодекси за поведение, техните изменения и допълнения в регистър и ги прави обществено достъпни чрез всички подходящи средства.

Като правен инструмент за международен пренос на данни към трети държави или международни организации одобреният кодекс за поведение трябва да бъде свързан със задължителни ангажименти с изпълнителна сила към администратора или обработващия лични данни в третата държава да прилага подходящите гаранции, включително по отношение на правата на субектите на данни. Спазването на кодексите за поведение задължително се наблюдава от компетентния надзорен орган и чрез механизъм за вътрешен контрол.

Мониторингът на конкретен кодекс на поведение може да се осъществява и от друга организация (частна или публична), която има съответно ниво на опит във връзка с предмета на кодекса и е акредитирана за тази цел от компетентния надзорен орган. Общите изисквания, на които трябва да отговаря акредитираната организация, са предвидени в Регламент (ЕС) 2016/679.[63] В случай че условията за акредитацията не са спазени, компетентният надзорен орган анулира акредитацията. Акредитираният орган може да предприема мерки в случай на нарушение на кодекса от страна на администратор или обработващ лични данни, включително като суспендира членството в кодекса или изключва от него съответния администратор или обработващ лични данни. Това не ограничава правомощията на надзорния орган да осъществява контрол върху изпълнението на задълженията, произтичащи от одобрения кодекс за поведение.

4.2.4. Сертифициране

Регламент (ЕС) 2016/679 предвижда възможността за приемане на механизми за сертифициране, печати или маркировки за защита на данните, чрез които да се демонстрира спазването на регламента. Тези механизми са насочени към администратори и обработващи лични данни, установени както на територията на ЕС/ЕИП, така и в трети държави. Целта на механизмите за сертифициране е да допринесат за правилното прилагане на регламента, като отчитат спецификите на отделните сектори. Надзорните органи и ЕКЗД трябва да насърчават приемането на механизми за сертифициране, печати и маркировки за защита на данните.

Механизмите за сертифициране заедно със съответните критерии се одобряват от компетентния надзорен орган или от ЕКЗД, като в тези случаи това може да доведе до единно сертифициране - "Европейски печат за защита на данните". Задължителни изисквания с оглед одобряването на даден механизъм за сертифициране е той да бъде доброволен и достъпен чрез прозрачна процедура. Той не може да бъде за срок по-дълъг от 3 години и не може да води до намаляване на отговорността на администраторите или обработващите лични данни. За да бъде основание за международен трансфер на данни към трети държави или международни организации, за които няма прието решение за адекватност на нивото на защита на данните, е необходимо в механизма за сертифициране да бъдат предвидени задължителни и изпълними ангажименти за администраторите и обработващите данни от съответната държава да прилагат предвидените правила, включително по отношение правата на субектите на данни.[64]

Компетентни органи да издават сертификати могат да бъдат компетентният надзорен орган или сертифициращите органи, които са получили необходимата акредитация. В съответствие с националното законодателство на държавата членка, сертифициращите органи е възможно да се акредитират от компетентния надзорен орган или от националния орган по акредитация, посочен в съответствие с Регламент

[63]Член 41, параграф 2 от Регламент (ЕС) 2016/679
[64]Член 46, параграф 2, буква е) от Регламент (ЕС) 2016/679

765/2008.[65] В България към момента такъв орган в съответствие с Регламент 765/2008 е Изпълнителна агенция „Българска служба за акредитация“.[66] Критериите за акредитация на сертифициращите органи се одобряват от компетентния надзорен орган или от ЕКЗД. Акредитацията се издава за максимален срок от 5 години, като може да бъде подновена. Изискванията за акредитация на сертифициращи органи, както и критериите за издаване на сертификати, одобрени от компетентния надзорен орган или от ЕКЗД, се оповестяват от надзорния орган. Комитетът обединява всички механизми за сертифициране, печати и маркировки в регистър и осигурява публичен достъп до тях. По повод на сертифицирането ЕК може да приема делегирани актове, за да уточни изискванията за сертифициране и за техническите стандарти за тях.

В случаите, когато се използват алтернативни механизми за гарантиране защитата на данните при международен трансфер, не е необходимо уведомление или разрешение от надзорен орган. Това до голяма степен облекчава администраторите и обработващите данни, като намалява административната тежест върху тях. Предварителното разрешение от компетентния надзорен орган остава необходимо единствено, когато предаването на данни към трети държави или международни организации става въз основа на договорни клаузи adhoc или за одобряване на административни договорености между публични органи и структури за защита на данните.

4.3. Дерогации

При липса на решение относно адекватното ниво на защита или подходящи гаранции, осигурени на основата на алтернативни механизми, предаването на данни към трета държава или международна организация може да се извърши единствено при наличието на предвидените в Регламент (ЕС) 2016/679 дерогации.[67] Такава възможност представлява например изричното съгласие на субекта на данните, като е необходимо то да бъде дадено след предоставяне на информация за рисковете. Освен това съгласието трябвада е свободно изразено, конкретно, информирано и недвусмислено, като може да бъде дадено посредством изявление или ясно потвърждаващо действие.[68]

Дерогации са предвидени във връзка с изпълнението на договори, по които страна е субектът на данните, ако са в негов интерес, както и когато трансферът на данни е необходим, за да бъдат защитени жизненоважните интереси на субекта на данните или на други лица. Ново основание за международен пренос на данни е предвидено за случаите, когато трансферът на данните е необходим с оглед законните интереси на администратора и те имат приоритет на правата и интересите на субекта на данните.[69] За да се приложи тази дерогация, трябва да няма възможност да се приложи друго основание, предаването на данни да е единично и да засяга ограничен брой субекти и администраторът да е предоставил подходящи гаранции във връзка със защитата на личните данни. Посочените по-горе дерогации не могат да се прилагат по отношение на дейности, извършвани от публичните органи при упражняването на техните публични правомощия. Предвижда се ЕКЗД да издаде насоки, препоръки и най-добри практики с цел допълнително да бъдат изяснени критериите и изискванията за предаване на данни при условията на дерогации.[70]

---

[65]Регламент (ЕО) № 765/2008 на Европейския парламент и на Съвета от 9 юли 2008 година за определяне на изискванията за акредитация и надзор на пазара във връзка с предлагането на пазара на продукти и за отмяна на Регламент (ЕИО) № 339/93 (Текст от значение за ЕИП),OJ L 218, 13.8.2008, p. 30–47

[66]www.nab-bas.bg

[67]Член 49, параграф 1 от Регламент (ЕС) 2016/679

[68]Член 4, параграф 11 от Регламент (ЕС) 2016/679

[69]Това основание е свързано със същите проблеми, които възникват при прилагането на основанието по член 6, параграф 1, б) е от Регламент (ЕС) 2016/679. Повече информация по прилагането на разпоредбата е достъпна в Toptchiyska, D. 2017. TheRuleofLawand EU Data ProtectionLegislation. ORBIT Journal. 1, 1 (Aug. 2017). DOI:https://doi.org/https://doi.org/10.29297/orbit.v1i1.16.

[70]Член 70, параграф 1, буква й) от Регламент (ЕС) 2016/679

5. Международно сътрудничество за защита на личните данни

С оглед важното значение на международния трансфер на данни за развитието на глобалния цифров пазар Регламент (ЕС) 2016/679 предвижда разпоредби, чрез които предоставя правомощия на ЕК и надзорните органи с цел улесняване на ефективното прилагането на законодателството за защита на данните. Тези правомощия включват предприемането на действия за разработването на механизми за международно сътрудничество с трети държави и международни организации, както и осигуряването на международна взаимопомощ при прилагането на законодателството за защита на личните данни. Намирането на хармонизирани решения на международно ниво за пренос на данни е свързано с необходимостта да се осигури правна сигурност и предвидимост, както и да се гарантира защитата на международно признатите етични ценности, свързани с правата на човека.

В своето Съобщение „Обмен и защита на личните данни в един глобализиран свят“ Европейската комисия предвижда конкретни мерки, които да осъществи в рамките на правомощията си в сферата на международното сътрудничество. Специално внимание се обръща на Конвенция 108 на Съвета на Европа, която е единственият международен инструмент в областта на защитата на данните с обвързващ характер и е отворена за държави извън организацията. ЕК си поставя за цел да подпомогне процеса на актуализиране на Конвенцията с оглед присъединяването на ЕС и трети държави към нея. Същевременно, за да постигне широк консенсус, свързан със защитата на личните данни в глобален план, ЕК планира сътрудничество с ООН, Г-20 и Организацията за Азиатско-тихоокеанско икономическо сътрудничество, както и други ключови международни партньори, с които да разработи механизми за международно сътрудничество. Чрез дейностите по международно сътрудничество ЕК си поставя за цел да съдейства за преодоляване на различията в регулирането на защитата на личните данни и гарантиране на висока степен на защита на данните в световен мащаб. Този подход ще подпомогне и улесни търговските предприятия, като им предостави възможност за по-ясно съпоставяне на различните системи и възможност да приемат съобразени с тях политики за защита на данните.

6. Заключение

Новият Регламент (ЕС) 2016/679 за защита на личните данни на ЕС си поставя за цел, от една страна, да осигури висока степен на защита на правата и в частност на личната неприкосновеност на физическите лица и, от друга страна, да осигури свободното движение на данни, което е необходимо не само с оглед на развитието на вътрешния цифров пазар, но и с оглед на тенденциите в глобалния икономически процес. Ефективността на модела за защита на личните на ЕС зависи от еднаквото и последователно прилагане на неговите правила на територията на всички държави членки на Съюза и също така от осигуряването на възможността данните на лицата от ЕС да бъдат предавани към трети държави и международни организации, при спазване на стандартите, предвидени в Регламент (ЕС) 2016/679. С оглед на това анализът и оценката на възможностите за международен трансфер на данни, съдържащи се в Регламента, е от изключително значение.

В сравнение с отменената Директива 95/46/ЕО новият Регламент предвижда по-ясни, по-детайлно регламентирани и по-разнообразни възможности за предаване на данни към трети държави и международни организации. Стандартите за признаване на адекватно ниво на защита в трета държава или международна организация са конкретно изброени, което създава яснота и предвидимост и ще подпомогне както ЕК в процеса на осъществяване на оценката, така и третите държави и международни организации, които имат интерес да получат съответното признаване. Също така изрично е предвидена възможността да бъде признавано т. нар. „частично“ адекватно ниво на защита както по

отношение на отделни територии, така и по отношение на конкретни сектори от икономиката, което ще даде възможност за повече гъвкавост при преценката с оглед постигане на ефективност.

Алтернативните механизми за международно предаване на данни дават възможност за конкретизиране на правилата, предвидени в Регламент (ЕС) 2016/679, което е предпоставка за създаване на правна сигурност и предвидимост. Същевременно многообразието от алтернативни механизми, включени в Регламента, дава възможност за избор на такъв, който най-ефективно би отговорил на нуждите на съответния отрасъл или група от предприятия. По отношение на стандартните договорни клаузи и задължителните фирмени правила с Регламент (ЕС) 2016/679 се разширява възможността за тяхното прилагане, а също така се премахва общото изискване за предварително уведомяване и разрешение от страна на надзорния орган, което намалява административната тежест по отношение на администраторите и обработващите данни. Кодексите за поведение и възможностите за сертифициране са нови инструменти за международен пренос на данни, чиято цел е да предоставят повече и по-гъвкави и адекватни възможности за предприятията, които осъществяват такъв пренос на данни. Разнообразието от дерогации, които са предвидени в Регламент (ЕС) 2016/679, също гарантира възможността за международен трансфер на данни при наличието на законно основание. По отношение прилагането на възможностите за международен трансфер на данни се очаква допълнителна правна регламентация от страна на ниво ЕС и на национално ниво, която да детайлизира и допълнително да изясни тяхното прилагане.

Предвидените в Регламент (ЕС) 2016/679 разнообразни възможности за международния трансфер на данни от страна на европейските и чуждестранните дружества в ЕС са предпоставка за улесняване и подпомагане на икономическите дейности. Същевременно приложимостта и ефективността на тези инструменти ще зависи от степента на координираност на действията на надзорните органи за защита на личните данни в ЕС, както и действията на ЕК и ЕКЗД не само в рамките на ЕС, но и с оглед осъществяване на международно сътрудничество в областта на защитата на данните.