ЗАЩИТА НА ДАННИТЕ ПО ПОДРАЗБИРАНЕ И НА ЕТАПА НА ПРОЕКТИРАНЕ В ЕПОХАТА НА ДИГИТАЛИЗАЦИЯТА

Венцислав Караджов
председател на Комисията за защита на личните данни
и заместник-председател на Европейския комитет
по защита на данните

DATA PROTECTION BY DEFAULT AND BY DESIGN IN THE AGE OF DIGITALISATION

Ventsislav Karadjov
Chairman Commission for Personal Data Protection
and Deputy Chair of the European Data Protection Board

Резюме: Концепцията на защита на данните по подразбиране и на етапа на проектиране е основополагаща за разбирането на съвременните процеси по защита на личните данни. Принципът *защита на данните на етапа на проектирането* е въведен да защити правата на физическите лица при автоматизирано обработване на лични данни. Той следва да намери отражение във всички съвременни проявления на дигитализацията, включително изкуствения интелект. Естествено негово продължение е защитата на данните по подразбиране.

Ключови думи: *лични данни, защита на данните, защита по подразбиране, защита на етапа на проектиране, дигитализация*

Abstract: The concept of data protection by default and by design is fundamental step for understanding contemporary personal data protection processes. The principle of "data protection by design" has been introduced to protect the rights of individuals in the automated processing of personal data. It should be reflected in all contemporary epitome of digitalisation, including artificial intelligence. Its continuation is the data protection by default.

Key words: *personal data, data protection, data protection by default, data protection by design, digitisation*

DOI: https://doi.org/10.36997/PPDD2021.9

Въведение

В последните три десетилетия, и най-вече през последните няколко години, личните данни на физическите лица все по-ясно и отчетливо се дефинират и налагат като защитимо право. На международно ниво Насоките на Организацията за икономическо сътрудничество и развитие (ОИСР) за защита на личните данни и задграничния им трансфер от 1980 г. (актуализирани през 2013 г.) и приетата малко след тях Конвенция на Съвета на Европа за защитата на физически лица по отношение на автоматизираното обработване лични данни (1981 г.) задават първоначалните стандарти за защита на личните данни при обработването им с автоматизирани средства.

Самото понятие за защита на данните на етапа на проектирането е разработено за приложение в дигиталния контекст на обработване на данни. Това е подход към разработване на информационни системи, изначално развит от г-жа Анн Кавукиан и формализиран през 1995 г. от съвместен доклад относно технологии за подобряване на поверителността на съвместен експертен екип на Комисаря по Информация и неприкосновеност на Онтарио, Нидерландския орган по защита на данните и Нидерландската организация за приложни научни изследвания. Правната рамка по защита на данните на етапа на проектирането е публикувана през 2009 г., а през следващата 2010 г. е приета и от Глобалната асамблея за защита на данните.

Защитата на данните на етапа на проектирането вменява задължението за включване на елемента за поверителност на данните през целия инженерен процес по разработване на дигитален продукт, т.е. защитата на данните следва да е концептуално заложен елемент в момента на разработване, а не нещо добавяно като допълнителна стойност при вече разработен и/или приключил дизайн на продукт. Този подход се възприема като *дизайн ориентиран към ценностите*, тъй като взема предвид общочовешките ценности по един ясно дефиниран начин през целия процес на разработване.

За описания времеви период се разви и процесът на дигитализация, който е една степен отвъд простото обработване на лични данни с технически средства. Дигитализацията по дефиниция е трансформация на всякакъв вид материална форма в поредица от знаци, предназначени за електронна обработка и предаване. В този контекст се

наложи и задълбочаване и детайлизиране на правните разпоредби за защита на данните, за да се отговори на настъпващата глобална дигитализация.

С въвеждането на изцяло новата правна рамка за защита на данните на ниво Европейски съюз, беше приет Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните, ОРЗД), който се прилага пряко от 25 май 2018 г. Това е нормативният акт, определящ правилата, свързани със защитата на физическите лица при обработването на личните им данни и относно свободното движение на тези данни. Общият регламент надгражда предишния режим за защита на данните, въведен от Директива 95/46/ЕО, транспонирана в българския Закон за защита на личните данни от 2002 г., като в същото време отчита динамиката на развитието на новите технологии и на дейностите по обработка на лични данни. Този акт има директно и пряко приложение по отношение на всички държави – членки на ЕС, като правата и задълженията, произтичащи от него, са приложими на недискриминационен принцип както по отношение на частноправни субекти, така и на публични организации. Тази правна реформа в рамката на ЕС включва и приемането на Директива (ЕС) 2016/680 на Европейския парламент и Съвета 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.

И двата европейски законодателни акта въвеждат изискването за защита на личните данни на етапа на проектирането и по подразбиране – съответно съображения 78 и 108 и чл. 25 от Регламент (ЕС) 2016/679 и съображения 53 и 55 и чл. 20 от Директива 2016/680. По този начин се обезпечава еднаквото и правилно прилагане на принципите за защита на неприкосновеността на личните данни на физическите лица както в чисто граждански и търговски аспект, така и в рамките на обработването на данни от правоприлагащи и правоохранителни органи. Този подход налага задължение на всеки администратор, обработващ лични данни, без значение от конкретната цел, за която той обработва данните, така да разработи и поддържа системите си, че да гарантира еднакъв, завишен и постоянен стандарт на защита.

Изложение

I. Защита на данните на етапа на проектиране

В рамките на Регламент (ЕС) 2016/679 защитата на данните на етапа на проектирането е базиран на седем *фундаментални принципа*:

- Проактивен, а не реактивен подход (превенция, а не последващо саниране).
- Настройката за поверителност да е зададена като default.
- Вграждане на поверителността в самия дизайн.
- Пълна функционалност – positive-sum, not zero-sum.
- Сигурност от край до край – пълен цикъл на защита.
- Видимост и прозрачност.
- Фокус към потребителя с уважение към поверителността му.

Технологиите за подобряване на поверителността дават възможност на ползвателите да защитят личната информация, която ги идентифицира, когато я предоставят или я управляват чрез услуги и приложения. Налице са много аспекти на защитата на данните на етапа на проектирането, включително при софтуерното разработване и инженерното разгръщане на системи, които включват административни елементи (например правна документация, политика за поверителност, процедури за преглед и при нарушение на сигурността), но предполагат и контрол в рамките на организацията, която използва технологията, както и адаптиране в контекста на конкретния бизнес процес. По този начин се налага да се вложат усилия за реализиране на принципа за справедлива информация, който да се внедри в дизайна и функционалността на информационните и комуникационните технологии. По този начин – при наличието на гаранции за поверителността на продукта от самото му разработване, администраторът на лични данни ще е в състояние (при спазване на принципа за защита на данните по подразбиране) да докаже, че обработва лични данни законосъобразно, в необходимия обем и без да ги съхранява за неприложим период от време.

Следва да бъдат установени отговорностите и задълженията на администратора за всяко обработване на лични данни, извършено от администратора или от негово име. По-специално, администраторът следва да е длъжен да прилага подходящи и ефективни мерки и да е в състояние да докаже, че дейностите по обработването са в съот-

ветствие с Регламент (ЕС) 2016/679, включително ефективността на мерките. Тези мерки следва да отчитат естеството, обхвата, контекста и целите на обработването, както и риска за правата и свободите на физическите лица.

Когато се обсъжда минимумът от отговорности и задължения на администратора на лични данни, те се обуславят от общите принципи за защита на данните (чл. 5 от Регламент (ЕС) 2016/679, а именно: законосъобразност, ограничаване на целите за обработване, свеждане на данните до минимум, точност, ограничение на съхранението, цялостност и поверителност, отчетност.

В този смисъл бизнес ориентираният подход на етапа на разработването на дигитален продукт би бил да се направи преглед, който да търси и да даде отговор на следните условия:

- Трябва ли наистина да събирам тези данни?
- Могат ли данните да бъдат анонимизирани или псевдонимизирани и да продължат да ми вършат работа?
- Какви други допълнителни данни могат да бъдат събрани и трябва ли да искам тези данни?
- Коя е заплахата?
- Какви категории или класове данни могат да бъдат засегнати?

Точно такъв подход ще гарантира и ориентирано към риска разработване, което да позволи и последващо актуализиране на технологията по начин, който ще създаде възможност за надграждане на защитата по обработване на данните по подразбиране (разглеждана по-долу). Понятието за риск за правата и свободите на физическите лица може да произтича от обработването на лични данни, което да доведе до физически, материални или нематериални вреди, да породи дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, накърняване на репутацията, нарушаване на поверителността на лични данни, защитени от професионална тайна, неразрешено премахване на псевдонимизация или други значителни, икономически или социални, неблагоприятни последствия. В подобни случаи субектите на данни могат да бъдат лишени от свои права и свободи или от упражняване на контрол върху своите лични данни, особено когато се обработват лични данни, които разкриват расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в професионална организация, както и обработването на генетични данни, данни за здравословното

състояние или данни за сексуалния живот или за присъди и нарушения, или за свързаните с тях мерки за сигурност.

Не на последно място е налице риск, когато се оценяват лични аспекти, по-специално анализиране или прогнозиране на аспекти, отнасящи се до представянето на работното място, икономическото положение, здравето, личните предпочитания или интереси, надеждността или поведението, местонахождението или движенията в пространството, с цел създаване или използване на лични профили. Специално внимание Регламент (ЕС) 2016/679 отделя на обработването на данни на уязвими лица, по-специално на деца, и в националното законодателство е въведено ограничение за обработване на такива данни на лица под 14- годишна възраст (чл. 25в от Закона за защита на личните данни). Когато обработването включва голям обем лични данни и засяга голям брой субекти на данни по дефиниция се приема, че е налице завишен риск за правата на физическите лица, което и налага подробен и ориентиран към защитата на поверителността дизайн.

Вероятността и тежестта на риска за правата и свободите на субекта на данни следва да се определят с оглед на естеството, обхвата, контекста и целта на обработването. Рискът следва да се оценява въз основа на обективна оценка, с която се определя дали операцията по обработването на данни води до *риск* или до *висок риск*. От тази оценка произтича и необходимостта от предварителна консултация с компетентен надзорен орган по реда на чл. 36 от Регламент (ЕС) 2016/679.

Инструмент, който е изключително полезен за администраторите на лични данни при спазването на изискванията на защита на данните на етапа на проектирането са Насоки № 4/2019 относно чл. 25 – Защита на данните на етапа на проектирането и по подразбиране на Европейския комитет по защита на данните, приети на 20 октомври 2020 г. В тях ясно е посочено, че задължение на администратора е да прилага подходящи технически и организационни мерки и необходимите гаранции в процеса на обработване.

В тези насоки ЕКЗД конкретно сочи, че дадена техническа или организационна мярка и гаранция може да включва всичко — от използване на усъвършенствани технически решения до основно обучение на персонала. Примерите, които могат да са подходящи в зависимост от характера на дейността, и рисковете, свързани със съ-

ответната операция по обработване, включват псевдонимизация на лични данни, съхранение на наличните лични данни в структуриран, широко използван и пригоден за машинно четене формат, предоставяне на възможност на субектите на данни да се намесват в дейността по обработване, предоставяне на информация за съхранението на лични данни, експлоатация на системи за откриване на зловреден софтуер, организиране на обучение на служителите по базова *кибер-хигиена*, въвеждане на системи за управление на неприкосновеността на личния живот и сигурността на информацията, въвеждане на договорни задължения за обработващите лични данни да прилагат определени практики за свеждане на данните до минимум и т.н.

Изрично се подчертава, че ефективността не изисква осъществяването на специфични технически или организационни мерки, т.е. прилагането на конкретен набор от мерки, а напротив, ефективността изисква да се докаже, че избраните мерки и гаранции са подходящи с оглед на прилагането на принципите на защита на данните в рамките на разглежданата дейност по обработване. Във връзка с това мерките и гаранциите следва да бъдат разработени така, че да са надеждни, а администраторът трябва да има капацитет да реализира допълнителни мерки, за да противодейства на възможно нарастване на нивото на риска. Следователно ефективността на мерките зависи от характера на конкретната дейност по обработване и от оценката на определени елементи, които трябва да се вземат предвид, когато се определят средствата за обработване.

Друг съществен елемент застъпен от ЕКЗД е практическото прилагане на критерия „достижения на техническия прогрес“, който се отнася не само до технологичните, но и до организационните мерки. Липсата на подходящи организационни мерки може да намали или дори изцяло да подкопае ефективността на избраната технология. Примерите за организационни мерки включват приемане на вътрешни политики, обучение, насочено към придобиване на актуални знания за дадена технология, сигурност и защита на данните, политики за управление на сигурността и административно управление на информационните технологии.

Пример: Използване на псевдонимизация (замяна на лично идентифицируем материал с изкуствени идентификатори) и криптиране (кодиране на съобщения така, че да могат да ги прочетат само оторизираните лица).

Важен елемент също така е определянето на *средствата за обработване*, които варират от общите до конкретните елементи при проектирането на обработването, включително архитектурата, процедурите, протоколите, оформлението и външния вид. Същевременно *моментът на определяне на средствата за обработване* се отнася до периода от време, когато администраторът взема решение относно начина на осъществяване на обработването и механизмите, посредством които ще се осъществи то.

Именно в контекста на горното се определя и, впоследствие, защитата на данните по подразбиране. Това обработване по подразбиране, което ще допълва и поддържа обработването на данни на етапа на проектиране, ще гарантира, че при едно добро планиране на защитата на данните на етапа на проектирането, последващото актуализиране ще гарантира все така завишено ниво на защита на неприкосновеността.

II. Защита на данните по подразбиране

Защитата на данните по подразбиране представлява принцип, според който администратор на лични данни обработва само данни, които са изрично необходими за всяка отделна цел, за която се обработват, без намесата на ползвателя на съответната технология. Съгласно тълкуването на ЕКЗД, понятието „по подразбиране“ при обработването на лични данни се отнася до определянето на стойности за конфигуриране или функции за обработване, които са зададени или предварително определени в рамките на система за обработване, като например софтуерно приложение, услуга или устройство, или процедура за ръчно обработване, които оказват въздействие върху обема на събраните лични данни, обхвата на тяхното обработване, периода на тяхното съхранение и тяхната достъпност. Администраторът следва да отговаря за въвеждането на такива настройки и опции „по подразбиране“, които да позволяват само обработване, което е строго необходимо за постигане на определената законосъобразна цел.

В контекста на дигитализацията има няколко практични стъпки, които ще гарантират, минимум, че обработването отговаря на изискването „по подразбиране“:

- Необходими ли са ми данните, които обработвам?
- Колко дълго се обработват личните данни?
- Кой има достъп до тези данни?

Администраторите следва да вземат предвид както обема на личните данни, така и видовете, категориите и нивото на детайлност на личните данни, необходими за целите на обработването. Когато събират големи обеми от лични данни, на етапа на проектирането те трябва да отчетат увеличения риск за принципите на цялостност и поверителност, да сведат данните до минимум и да ограничат съхранението, както и да го сравнят с намаления риск при събиране на намалени обеми и/или не толкова подробна информация за субектите на данни.

За описаните по-горе цели е неизбежно администраторът на лични данни да прави периодичен преглед и актуализация на настройките на изпитваната програма, приложение и т.н., както и да актуализира политиките си за поверителност, успоредно с напредъка на технологиите, които използва. Като примери в тази насока могат да се използват актуализирането на настройките „по подразбиране“ относно периодите за съхранение на данните в зависимост от варирашите изисквания за допустимите срокове за съхранение.

Особено съществен елемент при защитата по подразбиране е достъпността на данните и, в частност, контролът на достъпа до тези данни през цялото време на обработване. Дигитализацията като цяло предполага свързването на множество софтуерни продукти и предаването на данни чрез тях, в този смисъл, както и ЕКЗД подчертава, че без изрична човешка намеса/контрол, личните данни не трябва да бъдат достъпни за неограничен брой физически лица. По подразбиране администраторът трябва да ограничи достъпа и да предостави на субекта на данните възможност да се намеси, преди да публикува или по друг начин да предостави лични данни за субекта на данни на неограничен брой физически лица.

Предоставянето на достъп до лични данни на неограничен брой физически лица може да доведе до още по-широко разпространение на данните от предвиденото. Това е от особено значение при използването на интернет търсачките. Следователно, по подразбиране, администраторите следва да предоставят на субектите на данни възможност да се намесят, преди техните лични данни да бъдат предоставени за свободен достъп в интернет. Това е от особена важност, когато става дума за деца и лица от уязвими групи, както беше посочено и по повод рисковете на етапа на проектирането, които са приложими в цялост и при разработване на системата за поверителност

по подразбиране.

Пример: Социална медийна платформа трябва да се насърчи да зададе такива настройки на потребителските профили, които са най-благоприятни за неприкосновеността на личния живот, като например ограничи от самото начало достъпността до потребителските профили, за да не бъдат достъпни по подразбиране за неопределен брой лица.

Заключение

От особено значение и за двете системи за гарантиране на високо ниво на защита на личните данни е предоставянето на информация на крайния потребител. Част от принципите на *дизайн, ориентиран към ценностите* е зачитането на информираността на субектите на данни. От администраторите се дължи открита, ясна и точна информация какви данни ще бъдат обработвани, как ще се събират и обработват и ще бъдат ли предавани на трети лица. За тази цел ЕКЗД извежда в цитираното становище няколко основни принципа:

- яснота: информацията трябва да е представена на ясен и достъпен език, да бъде кратка и разбираема;
- смисъл: съобщенията следва да имат ясно значение за конкретната аудитория;
- достъпност: информацията трябва да е лесно достъпна за субекта на данните;
- контекст: информацията следва да е предоставена в правилния момент и в подходяща форма;
- уместност: информацията следва да е съотносима и приложима към конкретния субект на данни;
- универсална форма: информацията трябва да бъде достъпна за всички субекти на данни, да включва използване на подлежащи на машинно четене езици, за да се улесни и автоматизира четимостта и яснотата;
- разбираема: субектите на данни трябва да разбират достатъчно добре какво могат да очакват във връзка с обработването на личните им данни, особено когато става дума за деца или членове на други уязвими групи;
- различни комуникационни канали: информацията трябва да се предоставя чрез различни канали и медии, не само чрез писмен текст,

за да повиши вероятността за реално достигне на информацията до субекта на данните;

• структурирана в различни нива: информацията следва да бъде структурирана в различни нива по такъв начин, по който да бъде преодоляно противоречието между изисквания за пълнота и разбираемост, като същевременно се вземат предвид разумните очаквания на субектите на данни.

Използвана литература

Европейска комисия. (н.д.). Какво означава защитата на данните „на етапа на проектирането“ и „по подразбиране“? (https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_bg, 27.09.2021).

Evropeyska komisia. (n.d.). Kakvo oznachava zashtitata na dannite „na etapa na proektiraneto“ i „po podrazbirane“? (https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_bg, 7.09.2021).

Европейски комитет по защита на данните (2019). Насоки № 4/2019 относно член 25 Защита на данните на етапа на проектирането и по подразбиране. Брюксел: Европейски комитет по защита на данните.

Evropeyski komitet po zashtita na dannite (2019). Nasoki № 4/2019 otnosno chlen 25 Zashtita na dannite na etapa na proektiraneto i po podrazbirane. Bryuksel: Evropeyski komitet po zashtita na dannite.

Проект № 2007CB16IPO007-2011-2-06 Дигитална култура за регионално сближаване, съфинансиран от ЕС чрез Програма за ТГС по ИПП № 2007CB16IPO007.

Proekt № 2007CB16IPO007-2011-2-06 Digitalna kultura za regionalno sblizhavane, safinansiran ot ES chrez Programa za TGS po IPP № 2007CB16IPO007.

A Guide to Privacy by Design (2019). Madrid: Agencia Espanola Proteccion Datos.

Giannakakis, I. (2019). Privacy by Design and By Default. A Practical Guide for the Digital Era.

Mauritius: LAP Lambert Academic Publishing.

Jason Cronk, R. C. C. (2018). Strategic Privacy by Design. Oberlin, Ohio: IAPP, p. 278.

Stallings, W. (2020). Information Privacy Engineering and Privacy by Design: Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices. Pearson Education Inc.

Resolution on Privacy by Design (2010). // 32nd International Conference of Data Protection and Privacy Commissioners. Jerusalem: Global Privacy Assembly.

За контакти: Венцислав Караджов
Комисията за защита на личните данни
e-mail: kzld@cpdp.bg