Общи методически указания
за прилагане на Регламент (ЕС) 2016/679 (Общ регламент относно защитата на данните/ GDPR), в т.ч. и във връзка с обмена на данни между Министерството на образованието и науката (МОН) и прилежащите му централни и регионални структури и образователни институции

Общият регламент относно защитата на данните въвежда нова правна рамка, която обогатява съществуващата към момента нормативна уредба с нови принципи и правила във връзка със защитата на личните данни на физически лица, които от 25 май започват да се прилагат директно във всички държави членки на ЕС, предоставяйки единен стандарт за защита на данните в рамките на ЕС.

Въпреки че в публичното пространство акцент се поставя върху драстично повишените административни санкции в случай на нарушение, Регламентът съдържа редица нови моменти, свързани с обработването на лични данни, въвеждайки необходимост от:

- спазване на принцип за отчетност, който изисква осигуряване на надлежно документиране - оставяне на т.нар. „документална следа“ – доказателство за извършените операции по обработване налични данни в рамките на ведомството;
- гарантиране на прозрачност при обработването на личните данни, което налага надлежното уведомяване на физическите лица относно категориите данни, които се обработват, целите на извършваното обработване, правата им в тази връзка и др.;
- гарантиране на адекватно ниво на защита на личните данни чрез въвеждане или актуализация на подходящи технически и организационни мерки;
- гарантиране на правата на субектите на данните чрез предоставяне на прозрачна информация, надлежно водене на комуникация и предоставяне на условия за упражняването на правата им - достъп до лични данни, право на възражение, коригиране и други.

Целта на настоящите методически указания е да се предоставят ключови насоки и разяснение във връзка с практическото прилагане на комплексните изисквания на Регламент (ЕС) 2016/679 от страна на прилежащите централни и регионални структури и образователни институции (заедно наричани „ведомствата“ или поотделно „ведомство“), като се засяга и обмена на данни между МОН и последните.

Настоящите методически указания представляват информационен документ и използваните примери не претендират за изчерпателност.

I. Предприемане на стъпки по привеждане на дейността на ведомствата в съответствие с изискванията на новия Общ регламент за защита на личните данни

С оглед осигуряване на съответствие с новата правна рамка, въведена с GDPR, и надлежното спазване на принципите за законосъобразно обработване на лични данни, е препоръчително всички ведомства да предприемат следните основополагащи стъпки по привеждане на дейността им в съответствие с набора от изисквания на Регламента:

1. ***Проучване и анализ на всички процеси по обработване на лични данни в рамките на организацията/структурата:***

На първо място следва да се извърши така наречената „инвентаризация“ на процесите по обработване, чиято цел е да се идентифицират всички процеси, при които се обработват лични данни. В рамките на ведомствата следва да се проследят реалните процеси и практики, свързани с обработването на лични данни, като за всеки отделен процес се очертаят категориите лични данни и категориите субекти на данни, за които се отнасят данните, както и целите и законовото основание по смисъла на чл. 6 от Регламента за обработване на лични данни. Освен това следва да се идентифицират и анализират правомощията/задълженията/ на лицата, които обработват лични данни, начинът на възлагане на обработване на лични данни на лица вътре във ведомствата и извън него, достъпът до тях и начинът на обработване на лични данни (с автоматични или неавтоматични средства).

Под термина обработване на лични данни следва да се разбира всяка операция или съвкупност от операции, извършвана с лични данни или набор от лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване. Така например попълването на лични данни на ученик в дневник е действие по обработване, както и изготвянето на трудов договор с учител.

С оглед пълното идентифициране на очертаните по-горе процеси следва лицата, които ще извършат анализ на процесите в организацията, да имат добри познания както относно специфичната дейност, извършвана от ведомството, така и в областта на защитата на лични данни. Съгласно дефиницията на Регламент 2016/679 „лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“), **пряко или непряко**, по-специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор (напр. IP адрес) или **по един или повече** признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице. Така например следва да се третират като лични данни образователно-квалификационна степен, заемана длъжност, предишен трудов опит, номер на банкова сметка, хронично заболяване, имена на родители.

Важно е да се отбележи, че всяка допълнителна информация, която се добавя (натрупва) към някакви лични данни (били те пряко или непряко идентифициращи субекта на данни), също са лични данни, тъй като водят до идентифицирането му.

След събиране на пълния набор от информация в хода на инвентаризацията, следва да се извърши и последващ анализ на:

1.1. основанията за обработването – дали например личните данни се обработват във връзка с изпълнение на законово задължение, което се прилага към ведомството (напр. провеждане на конкурс по Закона за държавния служител), или с оглед изпълнението на задача от обществен интерес или при упражняването на официални правомощия. Всички основания за обработване на лични данни са изчерпателно изброени в чл. 6, параграф 1, чл. 9, параграф 2, и чл. 10 от Регламент 2016/679. Всеки процес по обработване, който не се извършва на някое от посочените основания, е незаконосъобразен;

1.2. спазването на принципите, свързани с обработването на лични данни (законосъобразност, добросъвестност, прозрачност, ограничение на целите, свеждане на данните до минимум, точност, ограничение на съхранението, цялостност и поверителност, отчетност – чл. 5 от Регламент 2016/679);

1.3. предприетите технически и организационни мерки за защита на личните данни спрямо съответната категория (особено важно е определянето такива по

отношение защитата на специалните категории данни по чл. 9 от Регламент 2016/679). Пример за такива мерки е определянето на нива и роли на достъп на лицата до съответните категории лични данни, съобразено с техните длъжностни характеристики, определяне на места за съхранение на данните с контролиран достъп - достъп с код или ключ, предприемане на технологични решения за криптиране на данните и др.;

1.4. наличие на вътрешни правила, регламентиращи приложението на тези мерки;

1.5. определяне типа отношения с трети лица, свързани с обмен на данни (администратор – администратор, администратор – обработващ; обработващ – под-обработващ);

1.6. спазването на задължението за реакция при нарушение на сигурността на данните и други.

Идентифицирането и анализа на процесите по обработване на лични данни е предпоставка за определяне на следващите стъпки по прилагане на изискванията на Регламента, а именно предприемане на конкретни мерки по привеждане на ведомството в съответствие.

II. Предприемане на конкретни мерки по привеждане на дейността на ведомството в съответствие с изискванията на GDPR

Основните мерки, необходими за законосъобразното обработване на лични данни, които администратори и обработващи лични данни следва да ревизират, адаптират, предприемат или изготвят с оглед спазването на гореизброените изисквания, са следните:

1. Регистри по чл. 30 от Регламент 2016/679

Съгласно изискванията на чл. 30 от Регламент 2016/679, администраторите на лични данни следва да водят и редовно да актуализират вътрешни регистри по обработване на личните данни. Тези регистри заместват предходната регистрация в регистъра, поддържан от Комисия за защита на личните данни (КЗЛД). Регистрите, касаят дейностите, за които администраторът отговаря или когато е обработващ – дейности по обработване, извършени от името на администратора. Поради това е изключително важно да се направи преценка кои дейности се обработват от ведомството в качеството му на обработващ и кои в качеството му

на администратор. Необходимо е такъв регистър да се води по отношение на всеки основен процес по обработване на лични данни.

Регистърът по чл. 30 от Регламент 2016/679 наподобява регистрите, които са поддържани и към този момент в КЗЛД и включва следните основни реквизити:

1.1. име и координати за връзка на администратора и — когато това е приложимо — на всички съвместни администратори, на представителя на администратора и на длъжностното лице по защита на данните, ако има такива;
1.2. цели на обработването (например при обработването на лични данни на лица кандидати за работа, целта на обработването е подбор на персонал);
1.3. основание за обработване на лични данни (при сключен договор - изпълнение на предмета на самия договор. Следва да се обърне внимание, че субектът на данни (физическото лице) трябва да е страна по този договор);
1.4. описание на категориите субекти на данни и на категориите лични данни (пр. служители; посетители в сградата; външни изпълнители; деца; учители и др.);
1.5. категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации (напр. НАП, НОИ, лица, които получават данни по силата на договор – например застрахователни дружества);
1.6. когато е приложимо, информация предаването на лични данни на трета държава или международна организация, включително идентификацията на тази трета държава или международна организация, а в случай на предаване на данни, посочено в член 49, параграф 1, втора алинея от Регламент 2016/679 - документация за подходящите гаранции;
1.7. когато е възможно, предвидените срокове за изтриване на различните категории данни (съгласно нормативната уредба и/или установени вътрешни правила); Ако фиксирането на конкретни срокове за съхранение на лични данни е невъзможно, следва да се определят критериите, използвани за определяне на срок за съхранение;
1.8. когато е възможно, общо описание на техническите и организационни мерки за сигурност, посочени в член 32, параграф 1 от Регламент 2016/679.

Регистрите следва да се поддържат в писмена форма, включително в електронен формат, и да се предоставя достъп на КЗЛД до тях при поискване. Регистрите са един от

важните инструменти за спазване на принципа за отчетност, тъй като документират основните процеси по обработване на лични данни в рамките на ведомството и предоставят база за бъдеща проверка за съответствие с приложимите принципи и правила относно законосъобразното обработване на лични данни. Следва да се установи механизъм за проследяване на контролната версия на поддържаните регистри, който да гарантира интегритета на съставения документ и да създаде възможност за проследяване на възникващите промени в процесите по обработване на лични данни.

По отношение на процеса видеонаблюдение, извършван за целите, установени в Закона за частната охранителна дейност, осъществяван по силата на договор за охрана, следва да се има предвид, че регистър „Видеонаблюдение“ се поддържа от юридическото лице, извършващо охранителната дейност. В случаите на самоохрана, регистърът се води от администратора. Следва да се обърне внимание, че съгласно чл. 2, ал. 3, т. 2 от Закона за частната охранителна дейност, бюджетни организации по смисъла на Закона за публичните финанси, лечебни заведения, институции в системата на предучилищното и училищното образование, висши училища, както и стратегически обекти от значение за националната сигурност, с издаден лиценз за самоохрана по реда на Закона за частната охранителна дейност могат да извършват частна охранителна дейност по отношение на собственото си имущество.

Регламент 2016/679 по правило допуска администраторите на лични данни да не водят такива регистри, ако имат по-малко от 250 служители, освен ако не е налице някое от посочените по-долу обстоятелства. При наличието на кое да е от тях и дружества с по-малко от 250 служители трябва да водят регистри:

- рисково обработване;
- неспорадично обработване;
- обработване на специална категория данни (данни по чл. 9, параграф 1 от Регламент 2016/679[1]) или на данни за присъди и нарушения.

Тълкуването на тази норма сочи, че Регламентът изключва от задължението за документиране в регистри единствено спорадични операции по обработване, които протичат за кратък период от време и не създават рискове за субектите.

[1] Специална категория данни са лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице.

В насоките на КЗЛД „Десет практически стъпки за прилагане на Общия регламент за защита на данните“, публикувани на уебсайта на Комисията (https://www.cpdp.bg/index.php?p=element&aid=1110), също е посочено, че администраторите следва да водят регистри като стъпка десет „Документиране и отчетност“. В тези указания КЗЛД не е обвързала това задължение с брой служители на администратора. Ето защо е силно препоръчително воденето на регистри от всички ведомства относно основните дейности по обработване. Поради това броя на служителите във ведомството не следва да се ползва като определящ критерий за изпълнение на изискването за водене на регистри.

2. Оценка на въздействието върху защитата на данните

Съгласно чл. 35 от Общия регламент относно защитата на данните, оценка на въздействието върху защитата на данните се извършва, когато съществува вероятност определен вид обработване, по-специално при което се използват нови технологии, и предвид естеството, обхвата, контекста и целите на обработването, да породи висок риск за правата и свободите на физическите лица. Като администратор на лични данни, съответното ведомство следва да извърши оценка при необходимост, когато нова дейност, която извършва, попада в обхвата на дейностите, за които Регламентът за защита на личните данни или документи на КЗЛД изискват това.

3. Вътрешни правила/ Инструкция за техническите и организационни мерки за осигуряване на адекватно ниво на сигурност на данните

По силата на чл. 32 от Регламента 2016/679, администраторът на лични данни следва да въведе и приложи подходящи технически и организационни мерки за защита на данните. Такова задължение е установено у нас още в Наредба № 1 от 30 януари 2013 г.
за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни на КЗЛД (Наредба № 1).

Вътрешните правила относно приложимите техническите и организационни мерки за защита на личните данни целят да определят правила, мерки и процедури необходими за осигуряване на сигурността на данните. Към настоящия момент, изготвянето на тези Вътрешни правила може да се извърши съобразно разпоредбите на Наредба № 1, която от

25.05.2018 г. следва да се счита за отменена[2] и предстои да бъде актуализирана спрямо нововъведенията на Регламента и трансформирана в Методическо ръководство. В тази връзка ведомствата следва да изготвят такива Вътрешни правила за техническите и организационните мерки, в случай, че към момента не са имали такива налични, или да ревизират и адаптират съществуващите към насоките на КЗЛД.

Във Вътрешните правила (Инструкция) се описват правата и задълженията на длъжностното лице по защита на данните, задължения на служителите при обработването на лични данни, извършването на оценка на въздействие и определяне на нива на защита, списък на регистрите, които се водят от ведомството, отношения с обработващи лични данни, предприетите технически и организационни мерки, действия при аварии, произшествия, бедствия и нарушение на сигурността, упражняване на правата на субектите на данни, категории получатели, провеждане на периодични прегледи относно необходимостта от обработване на лични данни, както и за заличаването им и прочие.

4. Политика за защита на личните данни

С оглед изпълнение на задължението по чл. 13 и чл. 14 от Общия регламент относно защитата на данните, субектите на данни имат право да получат от администратора информация относно обработването на техни лични данни. В тази връзка е необходимо администраторите да изготвят такива документи във връзка с дейностите си по обработване и да сведат тези документи до знанието на субектите.

Всяко ведомство следва да има, на първо място, изготвена политика относно обработването на лични данни на служителите, която следва бъде връчена за преглед от тяхна страна. С оглед спазването на принципа за отчетност и гарантиране на това, че служителите се запознати с процесите по обработване на личните им данни, препоръчително е полагането на подпис на всеки от служителите в края на политиката.

Политика за защита на личните данни следва да бъде изготвена и в зависимост от категориите субекти, чиито лични данни се обработват в рамките на ведомството (напр. лица в системата на образованието, чиито данни се обработват от ведомството, външни изпълнители, учители, ученици и други). Този документ следва да се разпространи до

[2] Наредбата за отменяне на Наредба № 1 от 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни (ДВ, бр. 14 от 2013 г.) е приета с Решение на Комисията за защита на личните данни от 18.05.2018 г. и влиза в сила от 25 май 2018 г. (ДВ, бр. 43, 25.05.2018 г.).

конкретните категории субекти на данни - например посредством публикуването ѝ на уебсайта на ведомството, изготвяне на информационни брошури и табели и т.н. Важно е да се отбележи, че при изготвяне на политиката следва да се използва ясен и достъпен език, за да се гарантира че субектите на данни са добре информирани и запознати с правата си.

Политиката за защита на личните данни съдържа следните основни реквизити:

4.1. данните, които идентифицират администратора и координатите за връзка с него и, когато е приложимо, тези на представителя на администратора;

4.2. координатите за връзка с длъжностното лице по защита на данните, когато е приложимо;

4.3. категориите субекти на данните, които обхваща;

4.4. категориите лични данни, които се обработват (данни за физическа, физиологическа, икономическа, семейна, културна и прочие идентичност[3]);

4.5. целите на обработването, за което личните данни са предназначени;

4.6. правното основание за обработването (всички възможни основания за обработване на лични данни са посочени в чл. 6, чл. 9 и чл. 10 от Регламент 2016/679). Ако обработването се извършва въз основа на член 6, параграф 1, буква „е“) - „легитимен интерес“ изрично следва да се посочи какъв е този легитимен интерес, преследван от администратора или от трета страна;

4.7. предоставяне на лични данни и последици при отказ да се предоставят на съответното ведомство;

4.8. други източници, от които се получават лични данни, като държавни, общински и съдебни органи, синдикални организации, организации от структурата на образованието и други;

4.9. обработване на информация за субекта на данни от трети лица – обработващи лични данни[4];

4.10. получателите или категориите получатели на личните данни (напр. ДАЗД, Агенция за социално подпомагане, НОИ, НАП, Инспекция по труда, служби по трудова медицина, синдикални организации, други компетентни държавни, общински и съдебни органи, и други);

[3] Вж. определение за лични данни по-горе.

[4] Това са най-често лица, на които администраторът предоставя данните по силата на закона или поради наличието на договорни отношения.

4.11. когато е приложимо, намерението на администратора да предаде личните данни на трета държава или на международна организация, както и наличието или отсъствието на решение на Европейската комисия относно адекватното ниво на защита или в случай на предаване на данни, съгласно посоченото в чл. 46, чл. 47 или чл. 49, параграф 1, втора алинея от Регламент 2016/679, позоваване на подходящите или приложимите гаранции и средствата за получаване на копие от тях или на информация къде са налични.

В допълнение, с оглед спазване на принципите за добросъвестно и прозрачно обработване, администраторът предоставя и следната допълнителна информация на субектите на данни:

4.12. срокът, за който ще се съхраняват личните данни, а ако това е невъзможно - критериите, използвани за определяне на този срок;

4.13. правата на субектите на данни по отношение на личните данни (право на информираност, право на достъп, право на коригиране на данни, право на изтриване, право на ограничаване на обработването, задължение за уведомяване на субекта на данни, право на преносимост на данните, право на възражение, право на уведомяване при нарушение на информационната сигурност);

4.14. правото на жалба до надзорен орган;

4.15. съществуването на автоматизирано вземане на решения, включително профилиране, посочено в член 22, параграфи 1 и 4 от Регламент 2016/679, и поне в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните;

4.16. координати на надзорния орган в Република България, а именно КЗЛД;

4.17. случаи, в които могат да бъдат ограничени правата на лицата.

III. Във връзка с извършване на видеонаблюдение на обекти на ведомствата

Видеонаблюдението само по себе си представлява процес на обработване на лични данни, в резултат на който се извършва запис чрез техническите средства за

видеонаблюдение. Видеозаписите съдържат лични данни, които спомагат за идентифицирането на конкретно физическо лице, както посочва и КЗЛД в свои насоки относно видеонаблюдението.[5] Видеонаблюдението е законосъобразно в случаите, когато то се извършва от:

- търговци или юридически лица, както и техни звена за самоохрана, които са лицензирани за извършването на частна охранителна дейност;
- държавни институции, на които се налага да извършват видеонаблюдение за изпълнение на своите функции;
- във всички останали случаи видеонаблюдение може да бъде извършвано само при наличие на нормативно основание или при съгласие на наблюдаваните/ записваните лица.

В тази връзка, при извършване на видеонаблюдение на входове и изходи, подходите на сграда, общи и други помещения на ведомствата, следва субектите на данни да бъдат информирани **чрез поставянето на информационни табели**, на видно място, **относно извършваните дейности по видеонаблюдение**, без да е необходимо да се уточнява точното място на техническите средства за наблюдение.

Информационните табели следва да съдържат информация, подобна на тази, съдържаща се в Политиките за защита на лични данни.

В повечето случаи видеонаблюдението на общи помещения и пространства се извършва с охранителна цел. Ако целта на видеонаблюдението е контрол на работния процес и спазване на работното време, КЗЛД посочва, че извършването на видеозаписи чрез средства за наблюдение на работниците/служителите, е законосъобразно, в случаите в които администраторът има нормативно основание за това. В тази връзка е препоръчително да не се събира съгласие на служителите.

IV. Уреждане на отношенията с лица, с които се обменят данни

[5] „Видеонаблюдението", Комисия по защита на личните данни, достъпно на: https://www.cpdp.bg/?p=element&aid=424 . Следва да се има предвид и новия Закон за частната охранителна дейност в сила от 31.03.2018.

Едно от задълженията, въведени с новата правна рамка, е именно уреждане на отношенията с лица, с които се обменят лични данни. Очертават се най-общо три типа отношения: между двама администратори и/или администратори-обработващи, както и между обработващ - подобработващ.

По дефиниция **администратор** означава физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на лични данни; когато целите и средствата за това обработване се определят от правото на ЕС или националното право, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на правото на ЕС или националното право (например в различни устройствени правилници, приемани от Министерство на образованието и науката).

Обработващ означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора – например в случаите, когато регионални управления на образованието сключват граждански договори с оценителите за държавни зрелостни изпити по заповед на министъра.

В тази връзка, при обмен на данни между /с публични органи и др. под., **обменът на данни следва да е уреден в нормативен акт** и да се извършва съобразно предвиденото в нормативната уредба. Когато обаче е налице обмен на данни с юридически лица – субекти на частното право, отношенията по повод на о**бмена на данни следва да се уредят в договор или друг правен акт**. В тази хипотеза (юридическо лице, субект на частното право) независимо дали отношенията по повод на обмен на данни са уредени в нормативен акт, или договор следва да се заложат основни положения като:

1. видове лични данни, които се обработват;
2. субекти, за които се отнасят данните;
3. основание за обработване;
4. срок на обработването;
5. технически и организационни мерки, които се предприемат с оглед гарантиране на висока сигурност на личните данни;
6. подробно разписване на правата и задълженията на двете страни (администратор-администратор; администратор-обработващ).

Когато обработването се извършва въз основа на договор, тези отношения могат да се уредят чрез анекс или допълнително споразумение към договора (договори за видеонаблюдение, договори със застрахователни дружества, договори с лица, поддържащи информационни системи и прочие).

Препоръчително е в процедурите, провеждани по реда на Закона за обществени поръчки, да се изготвят договори между възложител-изпълнител, в които се взима предвид обработването на лични данни. В договорите с изпълнители следва да се посочва ясно и дали/какви процеси по обработване на данни ще бъдат извършени от подизпълнители.

В процедурите по реда на Закона за обществени поръчки следва да се уведомяват участниците за обработването на лични данни от страна на ведомството във връзка с провеждането на процедурата, и то не само по отношение представителите на юридически лица, участници в процедурата, но и по отношение личните данни на физическите лица, посочени в предоставената от участниците документация.

V. Въвеждане на процедура за уведомяване на надзорния орган и за съобщаване на субектите на данните за нарушение на сигурността на личните данни

Съгласно изискванията на чл. 33 от Общия регламент за защита на данните, при нарушения в сигурността на данните администраторът следва да уведоми надзорният орган (КЗЛД) за това нарушение, като спазва определени срокове и предоставя на КЗЛД определен набор от информация. Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, то трябва да бъде съобщено и на субектите на данните (чл. 34, Регламент 2016/679). С оглед на това се препоръчва въвеждането на процедура, която да съдържа ясни правила за действията, които следва да се предприемат в случай на нарушение на сигурността на данните, основните отговорници за извършването на дейностите при възникване на инцидент и техните роли, както и за сроковете, които е нужно да се спазват.

VI. Определяне на Длъжностно лице по защита на данните

Регламентът въвежда фигурата на Длъжностното лице по защита на данните, чието определяне е задължително за:

- публичен орган или структура, освен когато става въпрос за съдилища при изпълнение на съдебните им функции;
- администратори, чиято дейност, поради своето естество, обхват и цели, изискват редовно и систематично мащабно наблюдение на субектите на данни;
- администратори, чиито основни дейности се състоят в мащабно обработване на специалните категории данни и на лични данни, свързани с присъди и нарушения.

Длъжностното лице по защита на данните има набор от задължения, сред които:

1. да информира и съветва администратора или обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на нормативните актове за защита на личните данни;
2. да наблюдава спазването на правилата за защита на личните данни и на политиките на администратора или обработващия лични данни по отношение на защитата на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване, и съответните одити;
3. да предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава извършването на оценката;
4. да си сътрудничи с надзорния орган и да действа като точка за контакт по въпроси, свързани с обработването, включително предварителната консултация и по целесъобразност да се консултира по всякакви други въпроси;
5. да действа като точка за контакт за субектите на данни по въпроси, свързани с обработването на техните лични данни и упражняването на правата им съгласно Регламента, националното законодателство и другите приложими изисквания за защита на личните данни.

Съгласно Регламента, длъжностното лице по защита на данните може да бъде член на персонала на администратора или на обработващия лични данни, или да изпълнява задачите въз основа на договор за услуги. Регламентът предвижда възможността, при условие че администраторът е публичен орган, едно длъжностното лице по защита на данните да отговаря за няколко структури. В тези случаи при определянето на длъжностното лице следва да се отчита организационната структура и размер на администраторите.

Ако се вземе решение за назначаване на длъжностно лице като част от персонала, следва да се следи за избягването на конфликт на интереси. Лицето може да съвместява дейността си с други функции, единствено при условие че се гарантира, отсъствие на конфликт на интереси. Длъжностите, при които може да възникне конфликт на интереси при изпълнение на функциите, вменени на длъжностното лице по защита на данни, включват най-общо ръководни позиции като ръководител на отдел „Човешки ресурси“, ръководител на ИТ отдел, главен счетоводител, както и други функции по-надолу в структурата, в случай че те са свързани с определяне на целите и средствата за обработване на лични данни. Длъжностното лице трябва да е пряко подчинени единствено на ръководителя на ведомството. То не следва да бъде натоварено с взимането на управленски решения.

VII. Спазване на основните принципи, свързани с обработването на лични данни

Съгласно Общия регламент за защита на данните, личните данни следва да бъдат обработвани законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните.

1. **Добросъвестността** е водещ принцип на Регламента, който се изразява в това, че всеки процес по обработване на лични данни следва да съответства на преследвана цел, да не се обработва непропорционален обем от лични данни и да не навлиза прекомерно в личната сфера на субектите на данни. Така например след постигане на целта на обработване на лични данни, обработването им следва да се преустанови, като в някои конкретни случаи, данните трябва да се унищожат.

В рамките на държавната администрация, добросъвестно е обработването, което държи сметка за предвидените в нормативната уредба данни, които следва да се обработват. Всяко обработване на данни, което се отклонява от тези параметри, би било недобросъвестно (така например създаването и съхраняването на копия от лични карти и други копия от документи за самоличност е недопустимо, освен в случаите, когато това се изисква изрично от действащото законодателство (напр. по реда на Закон за мерките срещу изпирането на пари). Действащото законодателство, уреждащо държавната служба, позволява снемането на данни от лични документи, но не и създаването на копия).

Недобросъвестно (респ. незаконосъобразно) би било обработване, което се отклонява от първоначалните цели, за които данните са били събрани. Такова отклонение е допустимо само въз основа на съгласието на субекта или въз основа на законодателството. Така например лица, които не са били назначени в рамките на определен конкурс, не могат да бъдат включвани в база данни за последващи подбори, без да е искано тяхното съгласие.

Когато обемът от лични данни, необходим за постигане на целта на обработване, не е посочен в нормативен акт, следва лицата, които имат управленски правомощия (напр. директор) да упражняват контрол за спазването на принципа на добросъвестност. Тези лица следва да съблюдават принципа, като не изискват предоставянето/събирането на информация, надхвърляща целта на обработване. Лицата, упражняващи управленски правомощия, следва също да контролират дали подчинените им лица спазват указанията за спазване на принципа.

2. Принципът на **законосъобразност** е обвързан с обработването на лични данни въз основа на конкретно правно основание. За повечето категории лични данни (напр. имена, адрес, електронна поща, номер на банкова сметка и др. под.), правните основания са уредени изрично в чл. 6, параграф 1 от Общия регламент за защита на данните. За специалните категории данни, познати още като чувствителни данни (напр. данни за здравето), е необходимо да е налице някое от условията за обработване по чл. 9, параграф 2 от Регламента. Обработването на данни за присъди и нарушения и свързаните с тях мерки за сигурност следва да става при спазване на разпоредбата на чл. 10 от Регламента.

Всеки процес по обработване на лични данни трябва да е придружен с конкретна цел за обработването на личните данни и конкретно правно основание.

3. Принципът на **прозрачност** се изразява в предоставянето на информация в „кратка, прозрачна, разбираема и леснодостъпна форма“. Това изискване означава, че информацията следва да се предоставя на лицата по най-простия възможен начин, като се избягват сложни езикови конструкции. Информацията не трябва да бъде формулирана с абстрактни или двузначни термини, или пък да позволява различни интерпретации. Администраторите трябва да предоставят информацията и да водят комуникация със субектите на данни по ефикасен начин, в кратка форма, за да се избегне т.нар. „заливане с информация“ (или казано по друг начин – да се претовари лицето с информация).

4. Принципът на **„свеждане на данните до минимум“** се свърза с ограничаване на обработването им до необходимото във връзка с целите, за които се обработват: При входяща

кореспонденция, в случай че служител получи повече данни отколкото е необходимо, следва да се използват само тези данни, които са необходими за осъществяване на целите на обработване, а останалите следва да бъдат заличени, ако това е възможно. Така например, такива данни не могат да бъдат заличени от входяща кореспонденция, която задължително се завежда. При изходяща кореспонденция, в случай на предоставяне на данни до трети лица с оглед изпълнението на конкретни цели, следва да се изпраща само необходимия/ изискания набор от информация. Това касае както обмена на данни между институции, така и с контрагенти.

5. Принципът **„точност“** означава, че данните следва да бъдат поддържани в актуален вид. В тази връзка е препоръчително да се разработи методика за актуализиране на данните в рамките на процеса на обработване на лични данни.

6. Принципът **„ограничение на съхранението“** изисква от ведомствата да спазват установените срокове за съхранение на данните, и да не съхраняват данните за срок по-дълъг от необходимото за постигане на целите, за които се обработват личните данни. Същите следва да предвидят процедура за периодичен преглед на данни, която да гарантира, че при постигане на целите на обработването и/или отпадане на основанието, данните ще бъдат заличени.

7. Новият принцип **„отчетност“**, въведен с Регламента, е насочен към доказване и документиране на спазването на всички останали принципи относно обработването на лични данни, а именно принципът на:

- законосъобразност, добросъвестност и прозрачност;
- ограничение на целите;
- свеждане на данните до минимум;
- точност;
- ограничение на съхранението;
- цялостност и поверителност.

Администраторите на лични данни носят отговорност за спазването на изискванията за защита на личните данни и следва във всеки един момент да са в състояние да докажат това съответствие. Това означава, че всеки администратор трябва да е наясно какви данни се събират, как се събират и за какви цели, както и да имат разработени вътрешни механизми,

правила и писмени процедури, които да доказват как е осигурено спазването на правилата за защита на личните данни.

Едни от основните инструменти за спазване на принципа за отчетност са:

7.1. поддържане на регистри на дейностите по обработване съгласно чл. 30 от GDPR;

7.2. изготвяне на вътрешни правила/ Инструкция за техническите и организационни мерки за осигуряване на адекватно ниво на сигурност на данните, както и водене на списък всички релевантни документи, относими и издавани във връзка с приложението на Инструкцията, а именно заповеди, определящи достъп на лица да определени помещение, длъжностни характеристики на служители и прочие. Инструкцията, спомага и за доказването и съблюдаването на принципа на „цялостност и поверителност“.

7.3. изготвяне на вътрешни правила, установяващи правила за документооборот – същите дават представа, как документите влизат в организацията, как се разпределят, как се съхраняват, как излизат от организацията и прочие;

7.4. разработване и разпространение на Политики за защита на личните данни – по този начин се осигурява надлежно документиране на факта, че субектите на данни са уведомени относно личните данни, които се събират за тях, целите и основанията на тяхното обработване, сроковете за съхранение и правата на субектите (информацията по чл. 13 и чл.14 от Регламент 2016/679);

7.5. разработване на процедура за уведомяване на надзорния орган и за съобщаване на субектите на данните в случай на нарушение на сигурността на личните данни;

7.6. анализ и писмено уреждане на отношенията с лица, с които се обменят лични данни - между двама администратори и/или администратори-обработващи, както и между обработващ – подобработващ (вж. насоките по-горе);

7.7. определяне на Длъжностно лице по защита на данните, когато се изисква;

7.8. въвеждане на (писмени) процедури и/ или практики за обезпечаване на принципите за добросъвестност, за свеждане на данните до минимум, за ограничение на съхранението и точност. *Примери:*

7.8.1. установяване на срокове за съхранение на документи както на хартиен, така и на електронен носител, съдържащи лични данни и/или установяване на

критерии за съхранение на данните (напр. съобразяване на абсолютни давностни срокове);

7.8.2. методика за извършване на периодичен преглед относно необходимостта от обработване на лични данни с оглед спазването на установените срокове за съхранение и проверка за отпаднала необходимост от обработване;

7.8.3. процедура за изтриване/ унищожаване на носители на лични данни (включително на копия или работни екземпляри на документи, за които няма установени срокове и правила за съхранение, и за които целта за обработване е постигната);

7.8.4. процедури за коригиране на неточни данни;

7.8.5. процедура за архивиране и съхранение на хартиени и електронни документи (за електронни писма следва да спазва установени вътрешни правила);

7.8.6. разработване на други документи, доказващи спазването на изискванията на Регламента (осигуряването на валидни съгласия в хипотезите, в които е необходимо то да се събира от физическите лица за обработването на личните им данни (вж. насоките по-долу);

7.8.7. при извършване на видеонаблюдение - разработване на по-детайлни информационни табели, които включват информация за правата на субектите на данни;

7.8.8. разработване и приемане на вътрешни процедури за разглеждане и отговаряне на искания от физически лица за упражняване на правата им, както и информационни бюлетини за упражняване на правата им;

7.8.9. извършване на оценка на въздействието при наличие на висок риск за правата и свободите на физическите лица.

VIII. Права на физическите лица

С оглед необходимостта от гарантиране упражняването на правата на физическите лица във връзка с обработването на личните им данни, следва да се разработят и приемат вътрешни процедури за разглеждане и отговаряне на искания от физически лица за упражняване на правата им. Процедурите следва да включват информация за това към кого могат да се обърнат субектите на данни, срокове на разглеждане и прочие (чл. 12, Регламент 2016/679).

1. Каква информация трябва да се предостави?

Член 13 и 14 от Общия регламент за защита на данните определят каква информация трябва да се предостави на субектите на данни, чийто данни се обработват[6].

Следва да се обърне внимание и да се следи стриктно изпълнението на фактическия състав на разпоредбите на Регламента, касаещи правата на субектите на данни. Така например правото на лицата да „бъдат забравени“ не може да се упражнява спрямо информация, чието обработване е свързано със спазването на законово задължение, което се прилага спрямо администратора, или за изпълнението на задача от обществен интерес, или при упражняването на официални правомощия, които са предоставени на администратора, когато това е предвидено в законодателството.

2. Как трябва да се предостави информацията?

Общият регламент относно защитата на данните предвижда информацията да се предоставя както писмено, така и електронно. Целта е да се гарантира информираността на субектите на данни относно обработването на техни лични данни.

Препоръчително е ведомствата да обозначават ясно в свои документи (на електронен или хартиен носител) като например образци на заявления, искания, протоколи, декларации и други подобни, дали предоставянето на данните и/или документите е задължително, или е изцяло доброволно, както и последиците от отказ за предоставяне на данни. Ведомствата биха могли да разработят (в допълнение към Политика за защита на личните данни) и информационни бюлетини за упражняване правата на субектите на данни.

IX. Съгласието като правно основание за обработване на лични данни

Съгласието е част от правните основания за обработване на лични данни, уредени в чл. 6, параграф 1 от Регламент 2016/679.

Ведомствата **не следва да събират съгласие от физическите лица за дейност по обработване, за която е налице друго основание**. В най-честия случай това би било законово задължение или изпълнение на задача в обществен интерес и упражняване на официални правомощия. При необходимост от обработване на лични данни, основаващо се на

[6] Вж. Политика за защита на личните данни, описана по-горе.

съгласие, следва то да бъде съобразено с условията за предоставяне на съгласие съгласно чл. 7 и чл. 8 от Регламент 2016/679.

При публикуване на снимки на уебсайт на ведомството, в някои случаи се предвижда искането на изрично съгласие от субектите на данни, а в случай на публикуване на снимки на деца под 14 години, съгласието следва да бъде получено от родител или настойник.

Съгласие за публикуване на снимка може да не се изисква, когато:

- изображението е било направено в хода на обществената дейност на снимането лице, или на публично или обществено място;
- изображението на лицето е само детайл в произведение, показващо събрание, шествие или пейзаж;
- изобразеното лице е получило възнаграждение, за да позира, освен ако между автора и изобразеното лице е било уговорено друго.

При всички случаи лицата следва да бъдат информирани, че ще бъдат заснети и да се предостави възможност, същите да не бъдат включени в снимковия материал, ако изразят несъгласие.

X. Обработване на лични данни в рамките на проекти

Когато ведомството е пряк бенефициент и/или в рамките на партньорство по проект, финансиран по определен финансов механизъм и проектът включва обработването на голям обем от лични данни за по-продължителен период от време (повече от 12 месеца), то е препоръчително правилата относно създаването на регистри и политики за защита на лични данни да се предприемат спрямо основните процеси по обработване на лични данни в рамките на проекта.

Следва да се има предвид, че когато ведомството е в партньорство с други организации, отношенията между тези субекти на данни следва да се характеризират като такива от типа на съвместни администратори на данни. В тази хипотеза, съгласно чл. 26 от Регламента съвместните администратори трябва да определят по прозрачен начин съответните си отговорности за изпълнение на задълженията по регламента, по-специално що се отнася до упражняването на правата на субекта на данни и съответните им задължения за предоставяне на информацията, посочена в членове 13 и 14, посредством договореност

помежду си, освен ако и доколкото съответните отговорности на администраторите не са определени от правото на Съюза или правото на държава членка, което се прилага спрямо администраторите. В договорността може да се посочи точка за контакт за субектите на данни.

Създаването на политики за защита на лични данни следва да бъдат сведени до знанието на субектите на данни. Начините за разпространение на информацията следва да се изследват и определят за всеки конкретен случай (дали са потребители на информационна платформа, участници в събитие, и/или лица, които са сключили договор във връзка с изпълнението на проекта).

XI. Образци на документи, използвани от ведомството

Във всички образци на декларации, заявления, искания, протоколи и други формуляри (електронни и на хартия) на съответното ведомство, следва да се обозначи дали посочването/ предоставянето на съответните данни и/или документи е задължително или договорно изискване, или изискване необходимо за сключването на договор, или е изцяло доброволно, както и последиците от отказ за предоставяне на данни.

Забележка: горната насока се отнася до формулярите, които са под контрола на съответното ведомство.

При определяне на образци на документи, които са под контрола на съответното ведомство, в случаите когато ведомството има дискреция при определяне на категориите лични данни, които да се изискват от субектите на данни, същото следва да извършва преценка за спазване на принципите за добросъвестност, пропорционалност, свеждане на данните до минимум.