

ОБЩИ ПРАВИЛА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
на издателска група „Просвета“

СЪДЪРЖАНИЕ

1.	Личните данни и издателска група „Просвета“	2
2.	Общи и Специални правила за защита на личните данни	2
3.	Основни принципи при обработване на лични данни	3
4.	Правно основание за обработване на лични данни	3
5.	Длъжностно лице по защита на данните	4
6.	Лични данни, обработвани от издателска група „Просвета“	5
6.1.	Понятие за лични данни	5
6.2.	Понятие за обработване на лични данни	6
6.3.	Видове лични данни, които се обработват	6
6.4.	Предаване на данни в рамките на издателска група „Просвета“	6
6.5.	Предаване на данни към трети лица	7
6.6.	Предаване на данни в страни извън ЕС	7
7.	Права на субектите на данни	8
7.1.	Право на информация	8
7.2.	Други права	8
7.2.1.	Достъп до и копие от личните данни	8
7.2.2.	Коригиране на личните данни	8
7.2.3.	Изтриване на личните данни	9
7.2.4.	Оттегляне на съгласието	9
7.2.5.	Ограничаване на обработването на лични данни	9
7.2.6.	Право на преносимост на данните	9
7.2.7.	Възражение срещу обработване на лични данни	9
7.2.8.	Възражение срещу автоматизирано обработване	9
7.2.9.	Право на жалба	9
7.3.	Упражняване на правата от страна на субектите на данни	10
8.	Сигурност и поверителност при обработване на личните данни	10
8.1.	Ниво на въздействие и ниво на защита	10
8.2.	Технически и организационни мерки за защита на данните	11
8.2.1.	Технически и организационни мерки при ниско ниво на защита	11
8.2.2.	Технически и организационни мерки при средно ниво на защита	12
9.	Срокове за съхраняване на лични данни	13
10.	Процедури за унищожаване на лични данни	13
11.	Стратегия при нарушение на сигурността на личните данни	14
11.1.	Понятие за нарушение на сигурността на личните данни	14
11.2.	Вътрешно докладване	14
11.3.	Разследване и оценка на риска. План за действие	14
11.4.	Необходимост от уведомяване на КЗЛД за нарушението	15
11.5.	Необходимост от уведомяване на засегнатите лица	15
11.6.	Документиране на нарушенията	16

1. Личните данни и издателска група „Просвета“

Защитата на личните данни е една от основните ценности на съвременните европейски общества. Тази защита е осигурена от правото на Европейския съюз и от националните законодателства на държавите членки. Считано от 25 май 2018 г., защитата на личните данни се разширява и осъвременява в отговор на технологичния прогрес и все по-ускорения обмен на данни. Основание за това е влизането в сила на Регламент (ЕС) 2016/679 (Общ регламент за защита на личните данни) и измененията в националното ни право, които той налага.

В издателска група „Просвета“ ежедневно обработваме лични данни и ежедневно се грижим за тяхната защита.

На издателска група „Просвета“ доверяват личните си данни хора от сферата на образованието и други наши партньори, които правят възможна дейността ни, а именно:

- автори и експерти, които участват в създаването на учебници, учебни помагала, познавателни книжки и други образователни ресурси;
- директори, учители, други педагогически специалисти, служители от системата на образованието, които поръчват, използват или имат интерес към нашите издания;
- родители и други лица, които се интересуват и закупуват нашите продукти;
- педагогически специалисти, експерти и други лица, които участват в наши обучения, събития или проекти;
- нашите служители и кандидати за работа;
- доставчиците на различни услуги.

Отношенията на доверие с тези лица са решаващи за устойчивото ни развитие. Издателска група „Просвета“ се стреми да запази това доверие, като за целта въвежда и се придържа към прозрачни правила за отговорно обработване и защита на личните данни.

2. Общи и Специални правила за защита на личните данни

Настоящите Общи правила за защита на личните данни на издателска група „Просвета“ са обобщение на добрите практики, които се прилагат от всички членове на групата:

- „Просвета – София“ АД;
- „Просвета Либри“ ЕООД;
- „Просвета Азбуки“ ЕООД;
- „Просвета Плюс“ ЕООД;
- „Просвета България“ АД;
- Фондация „Просвета – София“.

От своя страна всеки член на издателска група „Просвета“ приема и спазва собствени Специални правила за защита на личните данни, които конкретизират и допълват настоящите Общи правила.

Общите правила и Специалните правила на съответния член на издателската група действат заедно. В съвкупност те представляват цялостната политика на съответния член на групата за защита на личните данни. За да изпълняват тази роля, те предвиждат правата на лицата по повод обработването на личните им данни, задълженията на нашите служители, клиенти и партньори във връзка с това, а освен това въвеждат редица технически, организационни и други мерки за защита на данните, които се прилагат от издателска група „Просвета“

съобразно изискванията на Регламент (ЕС) 2016/679. Пълна информация за защитата на личните данни от издателска група „Просвета“ можете да намерите на интернет адрес: <http://www.prosveta.bg/privacy>.

Всички членове на издателската група и техните служители поемат ангажимент за точно придържане към описаните правила и за отговорно обработване и защита на личните данни. Не трябва да забравяме, че всяко нарушение на правилата за защита на данните, освен че застрашава правата и интересите на лицата, до които данните се отнасят, може да има и допълнителни последици, като финансови загуби, налагане на регулаторни мерки и загуба на репутация за издателска група „Просвета“.

3. Основни принципи при обработване на лични данни

Издателска група „Просвета“ спазва следните принципи при обработване на лични данни:

- Данните се обработват **законосъобразно, добросъвестно и по прозрачен начин** по отношение на лицата, до които се отнасят;
- Данните се събират **за конкретни, легитимни цели** и не се обработват по начин, несъвместим с тези цели;
- Данните са **подходящи, свързани със и ограничени до необходимото** за целите, за които се обработват;
- Данните са точни и при необходимост се **привеждат в актуален вид**. Предприемат се разумни мерки за своевременното **изтриване или коригиране** на данни, които са неточни или непълни;
- Данните се съхраняват **само докато са необходими** за целите, за които са събрани и се обработват;
- Данните се **заличават или поправят** при обосновано поискване на лицата, до които се отнасят;
- Прилагат се подходящи **технически и организационни мерки** за защита на данните с цел предотвратяване на неоправомощен достъп, неправомерно обработване, случайна загуба или изтичане на данни. В случай на такива нарушения издателска група „Просвета“ взема подходящи мерки за тяхното преустановяване, създава организация в съответствие със законовите изисквания и сътрудничи с компетентните органи, ако е необходимо те да се намесят.

4. Правно основание за обработване на лични данни

Обработването на лични данни е правомерно само и доколкото е налице поне едно от следните правни основания:

А) Субектът на данните е дал свободно, конкретно, информирано и недвусмислено **съгласие** за обработване на данните му за една или повече конкретни цели.

- В електронна среда съгласието може да се даде напр. чрез отбелязване с отметка, избиране на технически настройки или друго изявление или поведение на субекта на данните, което ясно показва, че той е съгласен с предложеното обработване на неговите лични данни. Извън електронна среда съгласието се дава по друг подходящ начин.
- Съгласието за обработване на данните може да бъде оттеглено по всяко време, без това да води до каквито и да е негативни последици за субекта на данните;
- При обработване на лични данни на дете съгласието се дава от носителя на родителска отговорност;

Б) Обработването е **необходимо** за **изпълнението на договор**, по който субектът на данните е страна, или за предприемане на стъпки **по искане** на субекта на данните **преди сключване на договор**;

В) Обработването е **необходимо** за спазването на **законово задължение**, което се прилага спрямо член на издателска група „Просвета“;

Г) Обработването е **необходимо**, за да бъдат защитени **жизненоважните интереси** на субекта на данните или на друго физическо лице.

Д) Обработването е **необходимо** за целите на **легитимните интереси** на издателска група „Просвета“ или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете.

Като общо правило издателска група „Просвета“ ще се позовава само на едно основание за обработването на определени данни за определена цел. С оглед на това във всеки отделен случай издателска група „Просвета“ следва предварително да установи кое от горните основания за обработване може да намери приложение.

5. Длъжностно лице по защита на данните

В издателска група „Просвета“ работи Длъжностно лице по защита на данните, към което можете да се обърнете по всички въпроси, свързани със защита на личните Ви данни, които се обработват от издателската група. С Длъжностното лице по защита на данните можете да се свържете по следните начини:

Мила Кръстева

- адрес: гр. София, ул. „Земеделска“ № 2
- телефон: 0882 53 33 96
- електронна поща: privacy@prosveta.bg

Длъжностното лице по защита на данните има следните основни правомощия:

- Контролира спазването на законовите изисквания и на Общите и Специалните правила на издателска група „Просвета“ за защита на личните данни;
- Информира и съветва издателска група „Просвета“ и служителите, които извършват операции по обработване на данни, за техните задължения във връзка с обработването на данни; повишава осведомеността и обучава служителите, участващи в операциите по обработване;
- Възлага отговорности и извършва одити;
- Действа като лице за контакт за субектите на данни, които могат да се обърнат към Длъжностното лице по защита на данните по всички въпроси, свързани с обработването на данните им и за упражняване на техните права. Действа като лице за контакт за Комисията за защита на личните данни и сътрудничи с нея;
- Участва в извършването на оценка на въздействието (виж по-долу); съобразява рисковете, свързани с операциите по обработване, отчитайки естеството, обхвата, контекста и целите на обработването.

Длъжностното лице по защита на данните спазва поверителност при изпълнение на своите задължения.

6. Лични данни, обработвани от издателска група „Просвета“

6.1. Понятие за лични данни

Личните данни са много общо понятие, което трябва да се разбира в широк смисъл. Когато физическо лице, независимо кое е то, може потенциално да бъде идентифицирано въз основа на данни, които издателска група „Просвета“ обработва с помощта на автоматични средства, или, макар обработването да става с други средства, данните са или са предназначени да съставляват част от регистър, тези данни представляват лични данни и издателска група „Просвета“ взема мерки за тяхното законосъобразно обработване и защита.

Видовете данни, които сами по себе си или в комбинация позволяват идентифицирането на физическо лице, са например: име, адрес, телефонен номер, електронна поща, данни за електронна идентификация, номер на банкова сметка, снимки/изображения, звукозаписи, видеозаписи, ЕГН и други лични номера, възраст, пол, дата на раждане, място на раждане, гражданско състояние, националност, физически характеристики, характеристики на начина на живот и поведението, данни за семейството, данни за обучения, работа и др. Специални категории данни, като такива за расов или етнически произход, религиозни или философски убеждения, членство в синдикални организации, както и други видове чувствителни данни, поначало не може да бъдат обработвани. От това правило има изрично предвидени изключения.

Потенциално всяка информация за лицето може да представлява негови лични данни. За да се приеме такава информация за лични данни обаче е необходимо тя на практика да може да доведе до точната идентификация на лицето. Всъщност това е критерият, по който Общият регламент за защита на личните данни (GDPR) определя кои данни са обект на защита. Например, ако разполагате с информация за името и пола на лицето, това няма да е достатъчно, за да го идентифицирате сред цялото население на страната (и поради това информацията, с която разполагате, няма да представлява лични данни), но ако знаете освен това, че лицето например е служител на някой от членовете на издателска група „Просвета“, най-вероятно ще можете да го идентифицирате точно (и поради това информацията, с която разполагате, вече ще се счита за лични данни).

За да се определи дали лицето може да бъде идентифицирано, се държи сметка не само за данните, с които разполагате, но и за това какви допълнителни средства и каква допълнителна информация може разумно да бъдат набавени и да се използват с цел идентификация на лицето, като се отчита колко струва това, колко време би отнело, какво е състоянието на техниката и т.н. Например комбинацията от длъжност и компания макар и без посочване на име би отнела само няколко минути за онлайн идентификация – напр. чрез LinkedIn – кое точно е лицето, и поради това би се приела за лични данни.

Законовите изисквания за защита на данните не се прилагат за анонимна информация, т.е. по отношение на данни, които не са свързани с идентифицирано или подлежащо на идентифициране физическо лице, или данни, които са анонимизирани по такъв начин, че субектът на данните да не може вече да бъде идентифициран. Анонимизиране се нарича процесът на обезличаване на данните само в случай че начинът, по който става това, е необратим. Ако обаче интегритетът на данните може да се възстанови с помощта на допълнителни средства (включително ако тези средства са на разположение на трети лица), т.е. ако процесът е обратим, данните са само псевдонимизирани (пример за това е криптирането). Псевдонимизираните данни продължават да са лични данни. Псевдонимизирането се насърчава, тъй като е мярка за защита на данните, но за псевдонимизираните данни важат всички други изисквания за законосъобразно обработване на лични данни.

Със защита се ползват само данните на физически лица (само те могат да бъдат лични данни). Данните за юридически лица са извън обхвата на защита, освен ако те правят възможно да се идентифицира физическо лице.

6.2. Понятие за обработване на лични данни

Обработването на данни, също както и самите лични данни, е понятие, което е с широк обхват. За обработване се приема на практика всяка операция, свързана с данните – 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 комбинирание, ограничаване, изтриване или унищожаване.

6.3. Видове лични данни, които се обработват

Всеки от членовете на издателска група „Просвета“ обработва данни, необходими за неговата дейност, и които са съобразени с особеностите на тази дейност. Поради това членовете на групата могат да обработват различни видове данни. Настоящите Общи правила за обработване на данни на издателска група „Просвета“ не съдържат конкретно описание на видовете данни, обработвани от отделните членове на издателската група или описание на конкретните операции по обработване, които отделните членове на групата извършват. Не такова е предназначението на Общите правила. По-подробна информация за видовете данни, които се обработват от всеки член на издателската група, за операциите по обработване, които съответният член прилага, както и за други въпроси, свързани с обработването и защитата на личните данни от страна на всеки членове на издателска група „Просвета“, можете да намерите в неговите Специални правила за обработване на лични данни и по-конкретно там можете да намерите информацията относно:

- а) лицата, чиито лични данни се обработват от съответния член на групата;
- б) видовете обработвани лични данни;
- в) целите на обработване на личните данни;
- г) правното основание за обработване на лични данни;
- д) получателите на лични данни;
- е) срока на съхранение на личните данни;
- ж) начина на съхранение на личните данни;
- з) мерките за защита на личните данни.

Актуални текстове на Специалните правила можете да намерите на интернет адрес: <http://www.prosveta.bg/privacy>.

6.4. Предаване на данни в рамките на издателска група „Просвета“

Членовете на издателска група „Просвета“ си взаимодействат и понякога обменят помежду си личните данни, които обработват.

Така например „Просвета Libri“ ЕООД получава заявки за закупуване на електронни учебници, а с това и свързаните със заявката лични данни на лицата, които я правят. За да се придвижи заявката, част от данните се предоставят на счетоводния отдел на „Просвета –

София“ АД, който осигурява счетоводно обслужване на всички членове на групата на „Просвета“. Ако заявката е за печатни издания, част от личните данни се предоставят и на „Просвета България“ АД, отговарящо за складовата база на издателската група, с цел проверка на наличностите.

В тези многостранни отношения всеки участник в групата „Просвета“ може да има различна роля от гледна точка на обработването на лични данни, т.е. може да бъде:

- администратор на данните, който определя целите и средствата за обработване на данните;
- обработващ данните, който извършва обработване по възлагане на администратор, без само да определя целите и средствата за обработване;
- възможно е членове на издателската група да са и съвместни администратори, в случаите, в които заедно определят целите и средствата за обработване.

Какво е качеството на всеки член на групата при обработване на данните (администратор, обработващ или съвместен администратор), се преценява във всеки отделен случай.

Членовете на издателската група са подписали Рамково споразумение за обработване на лични данни, съдържащо информация за качеството на всеки член на групата при основните операции по обработване на лични данни в издателска група „Просвета“, както и разпределение на свързаните с това отговорности между отделните членове. Рамковото споразумение за обработване на лични данни е приложение към и неразделна част от настоящите Общи правила. То е достъпно на интернет адрес: <http://www.prosveta.bg/privacy>.

6.5. Предаване на данни към трети лица

Когато е необходимо за дейността им, членовете на издателска група „Просвета“ могат да предават част от личните данни към лица, които са извън групата. Данните могат да бъдат предавани на такива трети лица за целите на счетоводното обслужване, поддържането на бази данни, IT услуги, консултации с външни специалисти, реклама и други услуги, които обичайно се ползват или предоставят от издателската група. Получатели на данните са лицата, на които данните е необходимо да бъдат предоставени за целите на такива услуги. В горните случаи се осигуряват гаранции за защита на правата и законните интереси на субектите на данните, включително, че третите лица ще прилагат подходящи технически и организационни мерки за защита.

За целта третите лица, които получават лични данни от издателска група „Просвета“, поемат подходящи правни ангажименти за законосъобразно обработване на данните (клаузи за поверителност и защита).

6.6. Предаване на данни в страни извън ЕС

За целите на софтуерното обслужване на дейността „Просвета“ може да предава данни в страни извън ЕС. Получатели на данните са лицата, предоставящи съответните услуги. Към момента издателска група „Просвета“ предава на това основание данни към дружество, което предоставя услуги по софтуерно обслужване на търговската дейност, учредено и развиващо дейност в САЩ, и свързаните с него дружества.

Във всички случаи издателска група „Просвета“ се уверява, че получателите на данните спазват необходимите високи стандарти за защита на данните и ги обработват законосъобразно, респ. издателската група не осъществява трансфери, когато няма увереност, че личните данни ще бъдат защитени.

7. Права на субектите на данни

7.1. Право на информация

Ако издателска група „Просвета“ обработва Ваши лични данни, Вие имате право да получите информация за това. За целта можете да отправите искане за получаване на следната информация:

- какви са целите и правното основание за обработване на данните Ви;
- кои са обработваните категории Ваши данни;
- кои са получателите или категориите получатели, пред които са разкрити личните Ви данни;
- какъв е срокът за съхранение на данните Ви или критериите, по които се определя този срок;
- потвърждение, в случай че имате право да изисквате коригиране, ограничаване на обработката или изтриване на личните данни;
- съществуването на право на жалба до КЗЛД и нейните координати за връзка;
- кои са наличните данни в процес на обработка и какъв е техният произход.

Напомняме Ви, че по всички въпроси, свързани с обработването на личните Ви данни от издателска група „Просвета“, можете да се обърнете към Длъжностното лице по защита на данните на издателска група „Просвета“ или към съответния член на издателската група.

7.2. Други права

Ако сте лице, чиито лични данни се обработват от издателска група „Просвета“, Вие имате и право на:

7.2.1. Достъп до и копие от личните данни. При упражняване на това право можете да получите потвърждение дали личните Ви данни се обработват, и ако това е така, да получите достъп до тях. При поискване от Ваша страна издателска група „Просвета“ ще Ви предостави копие от личните Ви данни, които са в процес на обработване. За допълнителни възможности за достъп и получаване на копие от данните може да прочетете в т. 7.2.6 по-долу – „Право на преносимост на данните“. Ако при кандидатстване за работа сте представили оригинали или нотариално заверени копия на документи, удостоверяващи физическа или психическа годност, необходимата квалификационна степен и стаж за длъжността и ако не сте одобрен(а) за назначаване, може да поискате да получите обратно представените документи в 30-дневен срок от окончателното приключване на процедурата по назначаване;

7.2.2. Коригиране на личните данни. При упражняване на това право можете да изискате коригиране без неоснователно забавяне на неточните лични данни, свързани с Вас. Като се имат предвид целите на обработването, можете да изискате непълните лични данни, свързани с Вас, да бъдат попълнени;

7.2.3. Изтриване на личните данни. При упражняване на това право можете да изисквате изтриване на личните данни, свързани с Вас, ако (1) те повече не са необходими за целите, за които са били събрани или обработвани по друг начин, или ако (2) сте оттеглили съгласието си, когато обработването има за правно основание съгласие и няма друго правно основание за обработване, или ако (3) сте възразили срещу обработването и няма законни основания за обработването, които да имат преимущество, или сте възразили срещу тяхното обработване за целите на директния маркетинг, или ако (4) личните данни са били обработвани незаконосъобразно, или ако (5) личните данни трябва да бъдат изтрети с цел спазването на

законово задължение. Правото на изтриване на данните е ограничено, доколкото обработването на данните е необходимо (1) за упражняване на правото на свобода на изразяването или правото на информация, (2) за спазване на законово задължение или (3) за установяването, упражняването или защитата на правни претенции;

7.2.4. Оттегляне на съгласието. По всяко време можете да оттеглите съгласието си Вашите лични данни да бъдат обработвани, и в случай че издателска група „Просвета“ разчита единствено на съгласието като правно основание за обработване на данните, обработването ще бъде преустановено. Молим да имате предвид, че това не засяга законосъобразността на обработването въз основа на съгласие, преди то да бъде оттеглено;

7.2.5. Ограничаване на обработването на лични данни. Можете да искате ограничаване на обработване на данните, свързани с Вас, когато (1) оспорвате точността на данни – за срок, който позволява да бъде проверено оспорването Ви, или когато (2) обработването е неправомерно, но не желаете личните Ви данни да бъдат изтрети, а искате вместо това само да бъде ограничено използването им, или когато заявите, че изисквате данните за установяване, упражняване или защита на правни претенции (в тези случаи се ограничава изтриването като операция по обработване), или когато (3) сте възразили срещу обработване, основано на легитимен интерес – за срока, необходим за проверка дали интересът на издателска група „Просвета“ да обработва данните, има преимущество пред Вашия интерес данните Ви да не бъдат обработвани;

7.2.6. Право на преносимост на данните. При упражняване на това право можете да получите личните данни, които се отнасят до Вас, в структуриран, широко използван и пригоден за машинно четене формат, както и да изисквате от издателска група „Просвета“ да прехвърли тези данни на друг администратор, в случай че:

- данните са предоставени на издателска група „Просвета“ от Вас и
- правното основание за обработване е съгласие или договорно основание и
- данните се обработват по автоматизиран начин, и
- не сте служител на издателска група „Просвета“;

7.2.7. Възражение срещу обработване на лични данни. Можете да възразите срещу обработването на личните данни, които се отнасят до Вас, когато основанието за обработване е легитимният интерес на издателска група „Просвета“; в тези случаи издателска група „Просвета“ има право да обоснове наличието на преимуществен легитимен интерес;

7.2.8. Да не бъдете обект на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последици за Вас или по подобен начин Ви засяга в значителна степен, освен ако това е позволено от закона или е необходимо за сключването или изпълнението на договор, в който случай трябва да се осигури обработването на данните да включва човешка намеса;

7.2.9. Право на жалба. Ако считате, че правата Ви във връзка със защитата и обработването на личните Ви данни са нарушени, можете да подадете жалба в Комисията за защита на личните данни в едногодишен срок от узнаването на нарушението, но не по-късно от пет години от извършването му. Можете да влезете във връзка с Комисията, както следва:

Комисия за защита на личните данни

- адрес: гр. София, 1592, бул. „Цветан Лазаров“ № 2
- телефон: 02/91 53 518
- електронна поща: kzld@cpdp.bg
- интернет страница: www.cdpd.bg

Вместо това в горния случай можете да подадете жалба до съответния административен съд или до Върховния административен съд в съответствие с общите правила за подсъдност.

7.3. Упражняване на правата от страна на субектите на данни

За да упражните някое от горните права, следва да отправите съответно искане до издателска група „Просвета“. За целта можете да се обърнете към Длъжностното лице по защита на данните или до съответния член на издателската група. Молим в искането си да посочите:

- име, адрес и данни за идентифициране;
- описание на искането;
- предпочитана форма за комуникация и действия по чл. 15 – 22 от Регламент (ЕС) 2016/679;
- подпис, дата на подаване на заявлението и адрес за кореспонденция.

При подаване на заявлението от упълномощено лице молим да приложите пълномощни.

За Ваше улеснение сме подготвили формуляр за отправяне на искане по повод обработването и защитата на лични данните Ви от издателска група „Просвета“, който е приложение към настоящите Общи правила. Формуляра може да намерите на интернет адрес: <http://www.prosveta.bg/privacy>.

В 60-дневен срок от отправяне на искането издателска група „Просвета“ ще предприеме съответните действия, за което ще Ви информираме. В същия срок ще Ви информираме и ако предприемането на действия ще изисква повече време или ако не можем да удовлетворим искането Ви, като ще посочим причините за това.

Издателска група „Просвета“ съдейства при упражняване на правата на субектите на данни, освен ако докаже, че не е в състояние да идентифицира лицето, което е отправило искането. Когато издателска група „Просвета“ има основателни съмнения за самоличността на лицето, може да изиска допълнителна информация за потвърждаване на самоличността му.

Издателска група „Просвета“ извършва действия по повод исканията на субекти на данни безплатно. Когато исканията са очевидно неоснователни или прекомерни, по-специално поради своята повторяемост, издателска група „Просвета“ може: (а) да наложи разумна такса, като взема предвид административните разходи за предоставяне на информацията или за комуникацията, или за предприемането на исканите действия или (б) да откаже да предприеме действия по искането.

8. Сигурност и поверителност при обработване на личните данни

8.1. Ниво на въздействие и ниво на защита

С помощта на Длъжностното лице по защита на данните членовете на издателска група „Просвета“ периодично проверяват вида на обработваните от тях лични данни и характера на операциите по обработване. В зависимост от резултатите от проверката разделят операциите по обработване на данните в две категории в зависимост от рисковете за правата и свободите на субектите, които произтичат от тях, както следва:

- операции по обработване с ниско ниво на въздействие и
- операции по обработване със средно ниво на въздействие.

В зависимост от установеното ниво на въздействие, по отношение на съответните данни се прилага и подходящо ниво на защита:

- лични данни, за които се прилага ниско ниво на защита;
- лични данни, за които се прилага средно ниво на защита.

Ако при проверката се установи, че дадена операция по обработване води до висок риск за правата на субектите на данни, например поради това, че при нея се прилагат нови технологични разрешения, и при положение че издателска група „Просвета“ не може да ограничи този риск с подходящи мерки от гледна точка на налични технологии и разходи за прилагане, преди съответната операция по обработване ще се осъществи консултация с Комисията за защита на личните данни.

8.2. Технически и организационни мерки за защита на данните

Членовете на издателска група „Просвета“ прилагат подходящи технически и организационни мерки за защитата на личните данни, като прилагат установените добри практики, съобразяват разходите за въвеждане на мерките, естеството, обхвата, контекста и целта на обработването, както и вероятността за нарушаване на правата и свободите на субектите на данните и последиците от това.

По-долу са представени обобщено видовете мерки според определеното ниво на защита. Конкретизация на мерките, включително чрез определяне на отговорни лица за тяхното прилагане, се извършва чрез вътрешни заповеди.

8.2.1. Технически и организационни мерки при ниско ниво на защита:

а) физическа защита:

- данните се обработват в служебните помещения или в помещения с ограничен достъп; елементите на комуникационно-информационните системи се разполагат в служебните помещения или в помещения с ограничен достъп;
- помещенията, в които се съхраняват данните, се заключват, когато в тях няма лица, които да упражняват надзор;
- документите с лични данни се съхраняват в обособени шкафове;
- достъп до данните се предоставя само на лицата, на които това е необходимо, за да осигурят законосъобразното им обработване;
- осигуряват се подходящи пожарогасителни средства и оборудване на помещенията.

б) персонална защита:

- на лицата, които участват в операции по обработване на данни, се разяснява нормативната уредба в областта на защита на данните; тези лица се запознават със и приемат Общите правила за обработване на данните на издателска група „Просвета“ и Специалните правила за обработване на данните на отделните членове; разясняват им се опасностите, свързани с обработването на лични данни;
- лицата, които участват в операции по обработване на данни, поемат задължение за неразпространение на личните данни.

Издателска група „Просвета“ е изработила стандартна клауза в горния смисъл, чрез която отговорните лица поемат съответните ангажименти.

в) документална защита:

- всеки член на издателска група „Просвета“ води отделни регистри за обработваните от него лични данни;
- всеки член на издателска група „Просвета“ определя регистрите, които поддържа на хартиен носител;
- достъпът до регистрите се предоставя само на лицата, на които това е необходимо, за да осигурят законосъобразното обработване на данните;
- служителите на „Просвета“ са длъжни да не допускат нерегламентиран достъп до документи, с които те работят и които съдържат лични данни;
- личните данни се съхраняват в сроковете, определени от администратора;
- след изтичането на сроковете за съхранение на данните те се унищожават съобразно процедурите на администратора.

г) защита на автоматизирани информационни системи и/или мрежи:

- на лицата, които участват в операции по обработване на данни с автоматизирани средства, се разясняват начинът на действие на системите и рисковете при обработване на лични данни с тях;
- достъп до данните имат само лицата, на които това е необходимо за законосъобразното обработване на данните; лицата получават достъп до системите след идентифициране и автентификация; достъпът до данните се осъществява на различни нива (спазва се принципът need-to-know); предотвратяват се неоправомощен достъп и обработване на данните, включително при тяхното предаване;
- водят се записи (логове) за събиране, промяна, справки, разкриване, включително предаване, комбиниране и изтриване; записите за извършена справка или разкриване дават възможност за установяване на основанията, датата и часа на такива операции и доколкото е възможно – идентификацията на лицето, което е направило справка или е разкрило лични данни, както и данни, идентифициращи получателите на тези лични данни;
- оборудването и носителите на информация са защитени и достъпът до тях е ограничен;
- използват се защитени връзки между информационните системи;
- прилага се подходяща защита от компютърни вируси;
- създават се и се поддържат резервни електронни копия за възстановяване на данните; осигурява се възможност за възстановяване на системите в случай на технически отказ; осигурява се докладване за появили се функционални дефекти; не се допуска увреждане на съхраняваните лични данни вследствие на неправилно функциониране на системите;
- сроковете за съхранение на данните при обработване с автоматизирани средства съответстват на сроковете, приложими за данни на хартиен носител.

8.2.2. Технически и организационни мерки при средно ниво на защита:**а) физическа защита:**

- прилагат се всички мерки за физическа защита при ниско ниво на защита;
- определят се зоните с контролиран достъп, в които се обработват данните;
- определят се конкретни способности за физическа защита;

б) персонална защита:

- прилагат се всички мерки за персонална защита при ниско ниво на защита;
- лицата, които участват в операции по обработване на данни, участват в подходящи обучения, включително такива за реакция при нарушения на сигурността на личните данни;
- лицата, които участват в операции по обработване на лични данни, споделят критичната информация, която е необходима за защита на данните;

в) документална защита:

- прилагат се всички мерки за документална защита при ниско ниво на защита;
- достъп до регистрите се предоставя само на определени лица;
- не може да се правят копия от данните или такива копия да се разпространяват без разрешението на лице, на което е предоставен достъп до данните;

г) защита на автоматизирани информационни системи и/или мрежи

- прилагат се всички мерки за защита на автоматизирани информационни системи и/или мрежи при ниско ниво на защита;
- елементите на информационните системи се поставят в помещения с ограничен достъп;
- води се отчетност за поддържането и експлоатацията на елементите на информационните системи;

д) криптографска защита:

- прилагат се стандартните криптографски възможности на операционните системи;
- прилагат се стандартите криптографски възможности на системите за управление на базите данни;
- прилагат се стандартните криптографски възможности на комуникационното оборудване.

9. Срокове за съхраняване на лични данни:

Личните данни се съхраняват в следните срокове:

- в срока за съхранение, ако той е предвиден в действащото законодателство, или
- докато данните са необходими за упражняване на права или изпълнение на задължения на членовете на издателска група „Просвета“, или
- докато данните са необходими за осъществяване на връзка с автори, клиенти или партньори, включително за подготовка, създаване или разпространение на издания, както и за организиране или провеждане на обучения, семинари или проекти;
- личните данни на участници в процедури по подбор на персонала се съхраняват не повече от три години;
- в случай на правен спор, за който данните могат да имат значение – до приключване на спора с влязло в сила съдебно решение.

10. Процедури за унищожаване на лични данни

След изтичането на сроковете за съхранение или когато по друга причина е отпаднало основанието за обработване на данните, те се унищожават по сигурен начин. Хартиените носители на данни се унищожават с шредер. Данните на електронни носители се унищожават по начин, който не допуска тяхното възстановяване. Подлежащите на унищожаване данни се пазят в поверителност, включително в процеса на унищожаване, освен ако са взети други мерки за защита на правата и свободите на лицата, до които данните се отнасят. Във всички случаи се прилагат добрите практики за съответния случай, които да осигурят необратимо заличаване на данните.

11. Стратегия при нарушение на сигурността на личните данни

11.1. Понятие за нарушение на сигурността на личните данни

Това е нарушение, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни. За видове нарушения се приемат:

- нарушение на поверителността – осъществен е неправомерен или неразрешен достъп до данните;
- нарушение на наличността – не може да бъде осъществен достъп до данните, въпреки че те следва да бъдат обработвани;
- нарушение на целостността – данните са променени по неправомерен или неразрешен начин.

11.2. Вътрешно докладване

Всеки, на когото стане известно, че е възникнало нарушение на сигурността на личните данни, обработвани от членове на издателска група „Просвета“, е длъжен незабавно да съобщи за това на Длъжностното лице по защита на данните на издателската група. Съобщението трябва да включва точна информация, доколкото такава е известна на лицето, което докладва, за вида на нарушението, за това колко лица са засегнати, кога е установено нарушението, както и за името на докладващия и негови координати за връзка. Съобщаването за нарушението на Длъжностното лице по защита на данните може да стане чрез попълването и изпращането на Формуляр, който е неразделна част от настоящите Общи правила и е достъпен на интернет адрес: <http://www.prosveta.bg/privacy>, или по друг начин, избран от лицето, което прави съобщението. Данните за нарушението не се разгласяват на други лица, освен ако в противен случай би се задълбочило нарушението или би се затруднило преодоляването на неговите последици.

Длъжностното лице по защита на данните незабавно извършва предварителна проверка по съобщението и установява, доколкото обстоятелствата позволяват това, дали е възникнало нарушение на сигурността на личните данни, какъв е неговият вид и колко и кои са засегнатите лица. Веднага след това Длъжностното лице по защита на данните докладва за полученото съобщение и за резултатите от извършената предварителна проверка на ръководството на съответния член на издателска група „Просвета“, засегнат от нарушението, а ако засегнатите или потенциално засегнатите членове са повече – до ръководството на всеки един от тях.

Във всички случаи, ако по преценка на Длъжностното лице по защита на данните се налага да бъдат предприети незабавни мерки, които да предотвратят задълбочаване на нарушението или които могат да спомогнат за преодоляване на неговите последици, и ако по преценка на Длъжностното лице отлагането на такива мерки съществено би намалило ефективността им, Длъжностното лице предприема мерките в първия възможен момент. Всички предприети мерки се докладват на ръководството на засегнатите членове на издателската група.

11.3. Разследване и оценка на риска. План за действие

Длъжностното лице по защита на данните, заедно с ръководството на засегнатите членове на издателска група „Просвета“, извършва внимателна преценка и анализ на обстоятелствата, свързани с нарушението, и риска от него за правата и свободите на физическите лица. При необходимост за целта се ангажират и други (включително външни) специалисти. Изработва се план за бързо ограничаване и преустановяване на действието на нарушението и справяне с неговите последици. Целите на плана се степенуват по важност:

- защита на правата и свободите на засегнатите от нарушението физически лица, включително недопускане на задълбочаване на нарушението; недопускане да бъдат засегнати правата и свободите на други физически лица;
- възстановяване на състоянието на личните данни каквото е било преди възникване на нарушението;
- предотвратяване или ограничаване на материалните вреди.

От организационна и финансова страна се обезпечава своевременното и ефективно прилагане на плана. Неразделна част от настоящите Общи правила е алгоритъм (схема) за действие при нарушение на сигурността на личните данни. След справянето с последиците от нарушението се изработва стратегия и се вземат мерки за недопускане на бъдещи нарушения.

Ако нарушението е възникнало при обработващ данните, незабавно се уведомява и администраторът на данните и се създава нужната координация за действие.

11.4. Необходимост от уведомяване на КЗЛД за нарушението

В случай че нарушението на сигурността на личните данни създава вероятност от риск за правата и свободите на физическите лица, чиито данни са засегнати, Длъжностното лице по защита на данните организира уведомяването на Комисията за защита на личните данни (КЗЛД) за нарушението.

Длъжностното лице по защита на данните предварително съгласува уведомяването на КЗЛД с ръководството на съответния засегнат член на издателска група „Просвета“. Длъжностното лице уведомява КЗЛД за нарушението, ако счита това за необходимо за защита на правата и свободите на субектите на данни, независимо от становището на ръководството по този въпрос.

Уведомяването на КЗЛД следва да се извърши без ненужно забавяне и когато това е осъществимо – не по-късно от 72 часа след първоначалното узнаване на нарушението. Уведомяването на КЗЛД съдържа:

- общо описание на нарушението на сигурността на личните данни;
- описание на категориите и приблизителният брой на засегнатите лица и на категориите и приблизителният брой на засегнатите записи на лични данни;
- името и координатите за връзка с Длъжностното лице по защита на личните данни;
- описание на евентуалните последици от нарушението на сигурността на личните данни;
- описание на предприетите или предложените мерки за справяне с нарушението, включително мерки за намаляване на евентуалните неблагоприятни последици.

Когато няма възможност цялата информация за нарушението да бъде предоставена в цялост на КЗЛД, тя се дава поетапно без неоснователно забавяне.

Уведомяването на КЗЛД се извършва от администратора на данните.

11.5. Необходимост от уведомяване на засегнатите физически лица за нарушението

Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, Длъжностното лице по защита на данните, без ненужно забавяне и при спазване на приложимото законодателство, уведомява засегнатите физически лица. Длъжностното лице по защита на данните предварително съгласува уведомяването с ръководството на съответния засегнат член на издателска група „Просвета“. Длъжностното лице организира уведомяването на засегнатите физически лица за

нарушението, ако счита това за необходимо за защита на техните права и свободи, независимо от становището на ръководството по този въпрос.

Уведомяването става без неоснователно забавяне и съдържа следната информация:

- общо описание на нарушението на сигурността на личните данни;
- евентуалните последици от нарушението;
- предприетите мерки за справяне с нарушението;
- името и координатите за връзка с Длъжностното лице по защита на личните данни;
- какви действия могат самите субекти на данните да предприемат за защита на правата си.

Към уведомяване на физическите лица може да не се пристъпва, ако са предприети подходящи технически и организационни мерки, които да защитават в достатъчна степен правата им, или ако са взети мерки, които да гарантират, че вече няма вероятност да се осъществи високият риск за техните права и свободи.

Ако индивидуалното съобщаване за нарушението на всеки субект на данни изисква непропорционални усилия от страна на издателска група „Просвета“, може да се пристъпи към публично съобщение за нарушението, което се координира с КЗЛД.

11.6. Документиране на нарушенията

Издателска група „Просвета“ води регистър на нарушенията на сигурността на личните данни, възникнали при нейните членове, в който се съдържа следната информация:

- дата на установяване на нарушението;
- описание на нарушението – източник, вид и мащаб на засегнатите данни, причина за нарушението;
- описание на извършените уведомявания – на КЗЛД, евентуално – на засегнатите лица;
- предприетите мерки за предотвратяване и ограничаване на последиците за субектите на лични данни и за издателска група „Просвета“;
- предприетите мерки за ограничаване на възможността от последващи нарушения на сигурността.

