ПОЛИТИКА

НА
КОМИСИЯТА ЗА ЗАЩИТА ОТ ДИСКРИМИНАЦИЯ

ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ
ПО РЕГЛАМЕНТ (ЕС)2016/679

Комисията за защита от дискриминация (КЗД) със седалище и адрес на управление: гр. София - 1125, бул. „Драган Цанков“ 35 и имейл адрес: kzd@kzd.bg, прилага във взаимоотношенията си със служители и граждани настоящата Политика, която определя задълженията ѝ по отношение защитата на данните и правата на субектите на данни по отношение на техните лични данни съгласно Регламент (ЕС) 2016/679 за защита на данните (GDPR).

Системата за сигурност на информацията в КЗД има за цел да защитава служителите, партньорите и клиентите ѝ от незаконни или вредни действия на физически лица, пряко или косвено, съзнателно или несъзнателно, при обработката на информация и лични данни, които са на тяхно разположение, а също така и при употребата на определено оборудване за изпълнение на служебните им задължения.

Политиката се прилага при обработка на информация в рамките на всяка система или съхранявана на всякакъв носител, участващ в обработката на лични данни/информация в КЗД, независимо от това дали обработката на лични данни е свързана с вътрешни операции на КЗД или с външни отношения на КЗД с трети страни.

Настоящата политика се прилага и по отношение начина, по който служителите на КЗД използват оборудването и инструментите, с които разполагат за изпълнение на служебните им задължения.

Тази политика определя задълженията на КЗД по отношение на събирането, обработката, прехвърлянето, съхранението и унищожаването на лични данни, отнасящи се до субектите на данни. Процедурите и принципите, посочени тук, трябва да бъдат спазвани по всяко време от Комисията, нейните служители, изпълнители или други страни, които работят от името на КЗД.

Комисията за защита от дискриминация се ангажира не само с буквата на закона, но и със справедливото третиране на всички лични данни, като се зачитат законните права, неприкосновеността на личния живот и доверието на всички лицата, с които се занимава.

Комисията за защита от дискриминация, като администратор на лични данни по смисъла за Закона за защита на личните данни, събира и обработва определена информация за физически лица.

Тази информация може да се отнася до жалбоподатели, сигналоподатели, ответни страни, свидетели и други физически лица, с които Администраторът има връзка или иска да установи контакт.

Настоящата политика за защита на личните данни урежда как да бъдат събирани, обработвани и съхранявани личните данни, за да отговарят на стандартите в организацията на Администратора и да са в съответствие с правните изисквания.

Всяка информация/лични данни, които станат достъпни за служителите на КЗД при изпълнение на служебните им задължения, ако са свързани с КЗД и дейността й, се счита за собствена и поверителна информация на КЗД, като по този начин се подчинява на защита в съответствие с приложимите закони и правна уредба относно защитата на поверителна информация, търговска тайна и лични данни.

I. ПРАВНО ОСНОВАНИЕ

Настоящата политика за защита на личните данни („Политика“) се издава на основание Закона за защита на личните данни и подзаконовите му актове, така както се променят („Българското законодателство“), и Общия регламент относно защитата на данните (ЕС) 2016/679 (GDPR).

GDPR дефинира „лични данни" като всяка информация, отнасяща се до идентифицирано или подлежащо на идентификация физическо лице („субект на данни“). Физическо лице, което може да бъде идентифицирано, е човек, който може да бъде идентифициран пряко или непряко, по-специално чрез посочване на идентификатор като име, идентификационен номер, данни за местонахождението, онлайн идентификатор или един или повече фактори, специфични за физическата, физиологичната, генетичната, умствената, икономическата, културната или социалната идентичност на това физическо лице.

Българското законодателство и GDPR предвиждат правила как организациите трябва да събират, обработват и съхраняват лични данни. Тези правила се прилагат от Администратора независимо дали се касае за данни, които се обработват електронно, на хартия или на други носители.

За да бъде обработването на лични данни в съответствие с правните изисквания, личните данни се събират и използват основателно, съхраняват се сигурно и Администраторът предприема необходимите мерки, за да не бъдат обработваните лични данни обект на незаконосъобразно разкриване.

Администраторът на лични данни е запознат с и следва принципите, предвидени в GDPR:

- личните данни се обработват *законосъобразно, справедливо, добросъвестно и по прозрачен начин* по отношение субекта на данните;
- личните данни се събират *за конкретни, изрично указани и легитимни цели* и не се обработват по начин, несъвместим с тези цели; по-нататъшната обработка за целите на архивирането в интерес на обществото, научните или статистическите цели не се счита за несъвместима с първоначалните цели;
- личните данни са *подходящи, свързани с и ограничени до необходимото* във връзка с целите, за които се обработват;
- личните данни са *точни и при необходимост се поддържат в актуален вид;* трябва да се предприемат всички разумни стъпки, за да се гарантира, че личните данни, които са неточни, като се имат предвид целите, за които се орбатоват, се изтриват или коригират незабавно;
- личните данни се съхраняват във форма, която да позволява идентифицирането на засегнатите лица *за период, не по-дълъг от необходимото за целите, за които се обработват личните данни;* те могат да се съхраняват за по-дълги периоди от време доколкото ще се обработват единствено с цел архивиране за обществени интереси, научни или статистически цели при условие, че са изпълнени съответните технически и организационни мерки, изисквани от GDPR, за да се защитят правата и свободите на субекта на данни;

- личните данни са обработвани по *начин, който гарантира подходящо ниво на тяхната сигурност,* включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки.

II. ЦЕЛИ НА ПОЛИТИКАТА

Настоящата Политика цели Администраторът да:

- бъде в съответствие с приложимото законодателство по отношение на личните данни и да следва установените добри практики;
- установи механизмите за водене, поддържане и защита на отчетните регистри;
- установи задълженията на длъжностните лица, обработващи лични данни и/или лицата, които имат достъп до лични данни и работят под ръководството на обработващите лични данни, тяхната отговорност при неизпълнение на тези задължения;
- защитава правата на персонала и гражданите;
- бъде открит как съхранява и защитава личните данни на физическите лица;
- установи необходимите технически и организационни мерки за защита личните данни от неправомерно обработване (случайно или незаконно унищожаване, случайна загуба, неправомерен достъп, изменение или разпространение, както и от всички други незаконни форми на обработване на лични данни);
- бъде защитен при риск от нарушения.

III. ОБХВАТ

Настоящата Политика се прилага по отношение обработването на лични данни на физически лица, така както са описани в електронните отчетни регистри, установени в съответствие с тази Политика, Българското законодателство и чл. 30 от GDPR („Регистри на дейностите по обработване“).

IV. СЪБИРАНЕ НА ЛИЧНИ ДАННИ

Категории данни и субекти

„Лични данни“ са всяка информация, свързана с идентифицирано физическо лице или такова, което може да бъде идентифицирано (субект на данни), а именно:

КЗД като администратор събира лични данни по отношение на следните категории лица:

- служители на КЗД
- жалбоподатели
- сигналоподатели
- участници в производството пред КЗД
- участници в обществени поръчки
- страни по договори
- кандидати за работа

Администраторът събира личните данни във връзка със следните цели:

1. *За изпълнение на дейности*, свързани с:

- изготвяне на различни видове документи;
- за установяване на връзка с лицето за контакт по телефон, факс или по всякакъв друг законосъобразен начин;
- за изпращане на важна информация до субектите във връзка с промени в правилата, условията и политиките на Администратора и/или друга административна информация;

2. За статистически цели

КЗД държи лични данни, които са пряко свързани с нейните служители. Личните данни се събират, съхраняват и обработват в съответствие с правата на субектите на

данни и задълженията на КЗД по GDPR и тази Политика. КЗД може да събира, съхранява и обработва личните данни - идентификационна информация за служителите, като:

1. име
2. ЕГН
3. лична карта
4. данни за връзка – адрес, телефон
5. възраст
6. пол
7. образование
8. общ трудов, служебен и осигурителен стаж
9. банкова сметка за получаване на възнаграждението
10. здравен статус
11. данни за отпуск по болест
12. автобиографии, формуляри за кандидатстване, придружителни писма и други подобни документи
13. оценки, прегледи на ефективността и други подобни документи
14. данни за възнаграждението, включително заплати, увеличения на заплатите, бонуси, комисионни, извънреден труд, обезщетения и разходи
15. протоколи за дисциплинарни въпроси, включително доклади и предупреждения, официални и неформални
16. здравни досиета – КЗД притежава здравни досиета на служителите, които се използват за оценка на здравето им и за изясняване на всички въпроси, които могат да изискват по-нататъшно разследване. По-специално, КЗД поставя висок приоритет в поддържането на здравето и безопасността на работното място, насърчаването на равните възможности и предотвратяването на дискриминацията на основата на увреждане или други медицински състояния. В повечето случаи здравните данни за служителите попадат в дефиницията на GDPR за специални категории данни. Поради това всички данни, свързани със здравето на субектите на данните, ще бъдат събирани, съхранявани и обработвани стриктно в съответствие с условията за обработка на лични данни от специална категория. Лични данни от специална категория няма да се събират, съхраняват или обработват без изричното съгласие на съответното лице.

Личните и здравните досиета са достъпни и използвани само от Човешки ресурси и СТМ и не се разкриват на други служители, изпълнители или други страни, работещи от името на КЗД без изрично съгласие на субекта на данните, за който се отнасят тези данни, освен в изключителни случаи, когато благосъстоянието на субекта, за който се отнасят данните, е изложено на риск. Здравните досиета се събират, съхраняват и обработват само до степента, необходима, за да се гарантира, че служителите могат да извършват работата си правилно, законно, безопасно и без незаконни или несправедливи пречки или дискриминация.

Субектите на данни имат право да поискат от КЗД да не води здравни досиета за тях. Всички такива искания трябва да бъдат изпратени в писмен вид и адресирани до КЗД.

КЗД, чрез своите членове и служители, държи и работи с лични данни, свързани с подадените от граждани жалби и сигнали, както и със страните в производството по преписки пред КЗД, като:

1. име
2. ЕГН
3. лична карта
4. данни за връзка – адрес, телефон
5. възраст
6. пол
7. образование
8. религия
9. раса и/или етнос
10. лично и обществено положение

11. професия, опит, стаж
12. здравен статус
13. политически убеждения и принадлежност
14. формуляри, придружителни писма и други подобни документи;
15. подробности за жалбите, включително документални доказателства, протоколи от заседания, бележки, следвани процедури, резултати и др..

Събиране на данните

Личните данни за всяко лице се предоставят доброволно от самите лица и се събират от Администратора в изпълнение на нормативно задължение. Лицата се уведомяват за разпоредбите на тази Политика предварително или в момента на получаване на данните им.

V. ПРАВА НА СУБЕКТИТЕ НА ДАННИ

Прозрачност и условия за упражняване правата на лицата

Администраторът предоставя информация на лицата в кратка, прозрачна, разбираема и лесно достъпна форма, на ясен език.

Администраторът се стреми да гарантира, че лицата са запознати относно обработваните от него лични данни и че те са информирани и изцяло, и напълно разбират, че обработването е в съответствие с изискванията на GDPR и Българското законодателство.

Администраторът предоставя информацията на лицата писмено или по друг начин, включително, когато е целесъобразно, с електронни средства. Ако лицето е поискало това, информацията може да бъде дадена устно, при положение че идентичността на лицето е доказана с други средства.

Администраторът предоставя на лицата безплатно информация относно действията, предприети във връзка с искане относно правото им на достъп, коригиране, изтриване, ограничаване на обработването, преносимост, възражение и автоматизирано вземане на решения, без ненужно забавяне и във всички случаи в срок от един месец от получаване на искането.

При необходимост този срок може да бъде удължен с още два месеца, като се взема предвид сложността и броя на исканията. Администраторът информира лицето за всяко такова удължаване в срок от един месец от получаване на искането, като се посочват и причините за забавянето.

Когато съответно лице подава искане с електронни средства, по възможност информацията се предоставя с електронни средства, освен ако лицето не е поискало друго.

Ако Администраторът не предприеме действия по искането, той уведомява лицето без забавяне и най-късно в срок от един месец от получаване на искането за причините да не предприеме действия и за възможността за подаване на жалба до надзорен орган, и търсене на защита по съдебен ред.

Когато исканията на лицето са явно неоснователни или прекомерни, по-специално поради своята повтаряемост, Администраторът може да наложи разумна такса, като се имат предвид административните разходи за предоставяне на информацията или предприемането на исканите действия, или да откаже да предприеме действия по искането.

Право на информация и достъп

Всяко лице има право да получи от Администратора потвърждение дали се обработват лични данни, свързани с него и ако това е така, да получи достъп до данните и следната информация:

- целите на обработването;
- съответните категории лични данни;

- получателите или категориите получатели, пред които са или ще бъдат разкрити личните данни;
- когато е възможно, предвидения срок, за който ще се съхраняват данните, а ако това е невъзможно - критериите, използвани за определянето на този срок;
- съществуването на право да се изиска от Администратора коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със засегнатите лица, или да се направи възражение срещу такова обработване;
- правото на жалба до Комисията за защита на личните данни;
- когато личните данни не се събират от самите лица, всякаква налична информация за техния източник;
- съществуването на автоматизирано вземане на решения, вкл. профилирането и поне в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване на лицата.

Лицата, чиито данни се обработват, могат да направят заявки за достъп до обектите по всяко време, за да научат повече за личните данни, които КЗД държи за тях, какво правят с тези лични данни и защо.

Лицата, чиито данни се обработват, трябва да използват писмена заявка за достъп до данни, която изпращат на служителя за защита на данните в КЗД.

Отговорите обикновено се правят в рамките на един месец от получаването им, но срокът може да бъде удължен с до два месеца, ако достъпът до данни е сложен и/или са направени многобройни искания. Ако се изисква такова допълнително време, субектът на данните трябва да бъде информиран.

Всички получени заявки за достъп до данни се обработват от служителя на КЗД за защита на данните.

КЗД не начислява такса за обработка на нормални заявки. Запазва си правото да начислява разумни такси за допълнителни копия на вече предоставена информация на субект на данни и за искания, които са явно неоснователни или прекомерни, особено когато тези искания са повтарящи се.

Администраторът предоставя на лицето копие от личните данни, които са в процес на обработване. За допълнителни копия, поискани от лицата, Администраторът може да наложи разумна такса въз основа на административните разходи. Когато лицето подава искане с електронни средства, по възможност информацията се предоставя в широко използвана електронна форма, освен ако лицето не е поискало друго.

Право на коригиране

Всяко лице, чиито данни се обработват от Администратора, има право да поиска от него да коригира без ненужно забавяне неточните лични данни, свързани с него. Като се имат предвид целите на обработването лицето има право непълните лични данни да бъдат допълнени.

Право на изтриване (право „да бъдеш забравен“)

Всяко лице, чиито данни се обработват от Администратора, има правото да поиска от него изтриване на свързаните с лицето лични данни без ненужно забавяне, а Администраторът има задължението да изтрие без ненужно забавяне личните данни, когато:

- личните данни повече не са необходими за целите, за които са били събрани или обработвани по друг начин;
- лицето оттегли своето съгласие, върху което се основава обработването на данните и няма друго правно основание за обработването;
- лицето възрази срещу обработването и няма законни основания за обработването, които да имат преимущество;
- личните данни са били обработвани незаконосъобразно;
- личните данни трябва да бъдат изтрити с цел спазването на правно задължение, което се прилага спрямо Администратора;
- личните данни са били събирани във връзка с прилагането на услуги на информационното общество.

Когато Администраторът е направил личните данни обществено достояние и е задължен съгласно предходния параграф да изтрие личните данни, той като отчита наличната технология и разходите по изпълнението, предприема разумни стъпки, включително технически мерки, за да уведоми администраторите, обработващи личните данни, че засегнатото лице е поискало изтриване от тези администратори на всички връзки, копия или реплики на неговите лични данни.

Право на ограничаване на обработването

Всяко лице, чиито данни се обработват от Администратора, има право да изиска от него ограничаване на обработването, когато се прилага едно от следното:

- точността на личните данни се оспорва от лицето за срок, който позволява на Администратора да провери точността на личните данни;
- обработването е неправомерно, но субектът на данните не желае личните данни да бъдат изтрити, а изисква вместо това ограничаване на използването им;
- Администраторът не се нуждае повече от личните данни за целите на обработването, но субектът на данните ги изисква за установяването, упражняването или защитата на правни претенции;
- субектът на данните е възразил срещу обработването в очакване на проверка дали законните основания на Администратора имат преимущество пред интересите на субекта на данните.

Когато обработването е ограничено съгласно горния параграф, такива данни се обработват, с изключение на тяхното съхранение, само със съгласието на субекта на данните или за установяването, упражняването или защитата на правни претенции или за защита правата на друго физическо лице, или поради важни основания от обществен интерес.

Когато субект на данните е изискал ограничаване на обработването, Администраторът го информира преди отмяната на ограничаването на обработването

Задължение за уведомяване при коригиране или изтриване на лични данни или ограничаване на обработването

Администраторът съобщава за всяко извършено коригиране, изтриване или ограничаване на обработване на всеки получател, на когото личните данни са били разкрити, освен ако това е невъзможно или изисква несъразмерно големи усилия.

Администраторът информира субекта на данните относно тези получатели, ако субектът на данните поиска това.

Право на преносимост на данните

Субектът на данните има право да получи личните данни, които го засягат и които той е предоставил на Администратора, в структуриран, широко използван и пригоден за машинно четене формат и има правото да прехвърли тези данни на друг администратор без възпрепятстване от Администратора.

Когато упражнява правото си на преносимост, субектът на данните има право да получи пряко прехвърляне на личните данни от един администратор към друг, когато това е технически осъществимо.

Право на възражение

Субектът на данните има право, по всяко време и на основания, свързани с неговата конкретна ситуация, на възражение срещу обработване на лични данни, отнасящи се до него (когато обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия на Администратора, или обработването е за целите на легитимните интереси на Администратора или на трета страна), включително профилиране. Администраторът прекратява обработването на личните данни, освен ако не докаже, че съществуват убедителни законови основания за обработването, които имат предимство пред интересите, правата и свободите на субекта на данни, или за установяването, упражняването или защитата на правни претенции.

VI. ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ДАННИТЕ

Защитата на данните на хартиено копие, както и на електронен носител, от неправомерен достъп, повреждане, изгубване или унищожаване се осигурява посредством поредица от вътрешно регулирани технически и организационни мерки.

Всички лични данни, събрани и обработвани под каквато и да е форма, се подчиняват на изискванията на настоящата Политика и всяка нормативна уредба по отношение на събирането, обработването, защитата и задържането на личните данни, а съответните документи се съхраняват на безопасно място, определено от КЗД за период, предвиден от приложимите закони и/или посочен от КЗД.

Служителите нямат право да съхраняват никаква поверителна информация на своите устройства, с изключение на временно необходимата им за конкретна, свързана с работата, дейност. Цялата поверителна информация и информацията, необходима за лична идентификация, следва да се съхранява само в режим на облачно съхранение, одобрен от ИТ служителите на КЗД. Всяко изтегляне на такива файлове на местни устройства следва да се избягва и да се ограничава само до необходимост, свързана с обработката за целите на работата.

Достъпът до Интернет и операциите, извършвани от служителите там съгласно изискванията на приложимите закони и подзаконови актове, могат да бъдат филтрирани и наблюдавани от надлежно упълномощени ИТ служители на КЗД.

Всички мобилни преносими устройства (лаптопи, таблети, смартфони и др.), както и всички облачни места за съхранение на информация, следва да бъдат одобрени от ИТ специалисти и надлежно обезопасени, за да се предотврати неоторизиран достъп.

Забранява се използването на обществени устройства за достъп, освен ако не се касае за случай на критична и спешна необходимост, свързана с работата и съгласувана с прекия ръководител.

VII. ТРАНСФЕР НА ЛИЧНИ ДАННИ

Администраторът не осъществява и няма да осъществява трансфер на лични данни в страни, извън Европейския съюз.

VIII. НАРУШЕНИЯ. УВЕДОМЯВАНЕ ЗА НАРУШЕНИЯ

Нарушения

Нарушение на сигурността на данни възниква, когато личните данни, за които Комисия за защита от дискриминация отговаря, са засегнати от инцидент със сигурността, в резултат на който се нарушава поверителността, наличието или целостта на личните данни. В този смисъл, нарушение на данните възниква, когато има нарушение на сигурността, водещо до инцидентно или незаконно унищожаване, загуба, изменение, нерегламентирано разкриване на данни, които се предават, съхраняват или се обработват по друг начин.

Уведомяване за нарушаване на данните

Всички нарушения на лични данни трябва да бъдат съобщени незабавно на служителя по защита на данните.

Ако се случи нарушение на лични данни и това нарушение има вероятност да доведе до риск за правата и свободите на субектите на данни (напр. финансови загуби, нарушаване на поверителността, дискриминация, репутационни щети или други значителни социални или икономически щети), служителят по защита на данните трябва да гарантира, че Комисията за защита на личните данни е информирана незабавно за нарушението и при всички случаи в рамките на 72 часа, след като е узнато за него.

В случай че нарушаването на личните данни е вероятно да доведе до висок риск за правата и свободите на субектите на данни, служителят по защита на данните трябва да гарантира, че всички засегнати субектите на данни са информирани за нарушението директно и без неоснователно забавяне.

Известията за нарушаване на данни включват следната информация:

1. Категориите и приблизителния брой на засегнатите субекти на данни;

2. Категориите и приблизителния брой записи на лични данни;

3.Името и данните за контакт на служителя на КЗД за защита на данните (или друго звено за контакт, където може да се получи повече информация);

4. Вероятните последици от нарушението;

5. Подробности за взетите или предложени за предприемане мерки от страна на КЗД за справяне с нарушението, включително, когато е целесъобразно, мерки за смекчаване на евентуалните неблагоприятни последици.

Оценка на нарушенията

След като служителят за защита на данните в КЗД получи информация за извършено нарушение трябва да определи дали конкретното събитие представлява нарушение на лични данни и да уведоми ръководството на Администратора за събитието (в случай, че то не знае).

В случай на нарушение сигурността на личните данни, което може да породи риск за правата и свободите на физическите лица, Администраторът (чрез съответния служител), без ненужно забавяне и когато това е осъществимо – не по-късно от **72 часа** след като е разбрал за него, уведомява за нарушението **Комисията за защита на личните данни.**

Когато и доколкото не е възможно информацията да се подаде едновременно, информацията може да се подаде поетапно без по-нататъшно ненужно забавяне.

Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, Администраторът без ненужно забавяне, съобщава на субекта за нарушението.

Администраторът документира всяко нарушение на сигурността на личните данни, включително фактите, свързани с нарушението, последиците от него и предприетите действия за справяне с него.

IX. УНИЩОЖАВАНЕ

След изтичането на срока за съхранението им носителите на информация (хартиени и технически), които не подлежат на предаване в Националния архивен фонд могат да се унищожават.

След изтичане на срока за съхранение данните се унищожават възможно най-бързо посредством унищожаването на хартиените носители чрез шредиране, а на техническия носител – чрез заличаване и изтриване на съответните файлове от компютрите на КЗД.

Счетоводната информация, както и всички други сведения и документи от значение за данъчното облагане и задължителните осигурителни вноски се съхраняват от Администратора в следните срокове:

- ведомости за заплати – 50 години;
- счетоводни регистри и финансови отчети – 10 години;
- документи за данъчно-осигурителен контрол – 5 години след изтичане на давностния срок за погасяване на публичното задължение, с което са свързани;
- всички останали носители – 5 години.

X. ОТЧЕТНОСТ И ВОДЕНЕ НА ЗАПИСИ

Служителят за защита на данните на КЗД е отговорен заедно със служителя „Човешки ресурси“ за надзор върху изпълнението на тази Политика, както и с GDPR и други приложими закони за защита на данните.

КЗД трябва да води писмени вътрешни записи за събирането, съхраняването и обработката на лични данни, които включват следната информация:

- името на КЗД, нейния служител по защита на данните и всички приложими процеси за обработка на данни от трети страни;

- целите, за които КЗД събира, съхранява и обработва лични данни;
- подробности за категориите на личните данни, събрани, съхранявани и обработвани от КЗД, и категориите данни за служителите, за които се отнасят тези лични данни;
- подробности за всички прехвърляния на лични данни към страни извън ЕИП, включително всички механизми и предпазни мерки за сигурност;
- подробности за продължителността на съхраняването на лични данни от КЗД;
- подробни описания на всички технически и организационни мерки, предприети от КЗД, за да се гарантира сигурността на личните данни.

XI. МОНИТОРИНГ НА СУБЕКТИТЕ НА ДАННИТЕ

КЗД може от време на време да наблюдава дейностите на субектите на данни. Такъв мониторинг може да включва, но не непременно да се ограничава до интернет и електронно наблюдение. В случай че трябва да се извърши мониторинг от всякакъв вид (освен ако изключителни обстоятелства, като например разследване на престъпна дейност или въпрос с еднаква тежест, оправдават скрит мониторинг), субектите на данни за служителите ще бъдат информирани за точния характер на мониторинга в предварително.

Наблюдението не следва (освен ако изключителни обстоятелства го оправдават, както по-горе) да се намесва в нормалните задължения на служителя.

Наблюдението ще се извършва само ако КЗД счита, че е необходимо да се постигне ползата, която е предназначена да се постигне. Личните данни, събрани по време на всяко такова наблюдение, ще бъдат събирани, съхранявани и обработвани само по причини, пряко свързани с (и необходими за) постигането на планирания резултат и по всяко време, в съответствие с правата на субектите на данни и задълженията по Регламента.

КЗД трябва да гарантира, че няма ненужно навлизане на личните комуникации или дейности на субектите на данни и при никакви обстоятелства мониторингът няма да се извършва извън обичайното работно място на работното лице или работното време, освен ако съответното лице, използва служебно оборудване или други съоръжения, включително, но не само, имейл на КЗД, служебен интранет или виртуална частна мрежа (ВЧМ), предоставяна за използване от служителите.

XII. СИГУРНОСТ НА ДАННИТЕ

Прехвърляне на лични данни и съобщения

КЗД гарантира, че са предприети следните мерки по отношение на всички комуникации и други трансфери, включващи лични данни (включително, но не само, лични данни, свързани със служителите):

1. Всички имейли, съдържащи лични данни, трябва да бъдат шифровани;
2. Всички имейли, съдържащи лични данни, трябва да бъдат обозначени като „поверителни“;
3. Личните данни могат да се предават само чрез защитени мрежи; предаването на данни по необезпечени мрежи не е разрешено при никакви обстоятелства;
4. Личните данни не могат да се предават чрез безжична мрежа, ако има разумно приложима алтернатива;
5. Личните данни, съдържащи се в тялото на имейл, независимо дали са изпратени или получени, трябва да се копират от тялото на този имейл и да се съхраняват сигурно. Самият имейл трябва да бъде изтрит. Всички временни файлове, свързани с него, също трябва да бъдат изтрити;
6. Когато личните данни трябва да бъдат изпратени чрез факсимилно предаване, получателят трябва предварително да бъде информиран за предаването и трябва да чака от факс машината да получи данните;
7. Когато личните данни трябва да се предават на хартиен носител, те трябва да бъдат предадени директно на получателя или изпратени с помощта на услуга за доставка;

8. Всички лични данни, които трябва да бъдат прехвърлени физически, независимо дали са на хартиен носител или на подвижни електронни носители, се прехвърлят в подходящ контейнер, обозначен като „поверителна".

Съхранение

КЗД гарантира, че са предприети следните мерки по отношение на съхраняването на лични данни (включително, но не само, лични данни, свързани със служителите):

1. Всички електронни копия на лични данни трябва да се съхраняват сигурно, като се използват пароли и криптиране на данните;
2. Всички хартиени копия на лични данни, както и всички електронни копия, съхранявани на физически, подвижни носители, трябва да се съхраняват сигурно в заключена кутия, чекмедже, шкаф или други подобни;
3. Всички лични данни, съхранявани по електронен път, трябва да бъдат архивирани, със съхранени архиви [на място] и/или [извън]. Всички архиви трябва да бъдат шифровани;
4. Не трябва да се съхраняват лични данни на нито едно мобилно устройство (включително, но не само, лаптопи, таблети и смартфони), дали такова устройство принадлежи на КЗД или по друг начин без официално писмено одобрение на председателя; в случай на такова одобрение, стриктно в съответствие с всички указания и ограничения, описани в момента на издаване на одобрението, и не повече от абсолютно необходимото;
5. Лични данни не трябва да се прехвърлят на каквото и да е устройство, което е част от служител; лични данни могат да бъдат прехвърляни само на устройства, принадлежащи на работещи от името на КЗД, когато въпросната страна се е съгласила напълно да спази духа на тази политика и на GDPR.

Изхвърляне

Когато всички лични данни трябва да бъдат изтрити или изхвърлени по друг начин по каквато и да е причина (включително когато са направени копия и вече не са необходими), те трябва да бъдат напълно заличени и унищожени.

Използване на лични данни

КЗД гарантира, че са предприети следните мерки по отношение използването на лични данни:

1. Никакви лични данни не могат да бъдат споделяни неофициално и ако служител, изпълнител или друга страна, работеща от името на КЗД, изисква достъп до лични данни, до които те вече нямат достъп, този достъп трябва да бъде формално поискан.
2. Никакви лични данни не могат да бъдат прехвърляни на служители, изпълнители или други лица, независимо дали тези страни работят от името на КЗД или не, без разрешение на председателя на КЗД.
3. Личните данни трябва да се обработват с грижа по всяко време и не трябва да бъдат оставени без надзор.
4. Ако се разглеждат лични данни на компютърния екран и въпросният компютър трябва да остане без надзор за определен период от време, потребителят трябва да заключи компютъра и екрана, преди да напусне компютъра.
5. Когато личните данни, съхранявани от КЗД, се използват за маркетингови цели, отговорността се гарантира, че съответното съгласие е получено и че никой субект на данни за служителите не се е отказал пряко или чрез услуга от трета страна.

ИТ сигурност

КЗД гарантира, че са предприети следните мерки по отношение на ИТ и информационната сигурност:

1. Всички пароли, използвани за защита на личните данни, трябва да се променят редовно и не трябва да използват думи или фрази, които лесно могат да бъдат познати или компрометирани по друг начин. Всички пароли трябва да съдържат комбинация от главни и малки букви, цифри и символи.
2. При никакви обстоятелства пароли не трябва да се записват или да се споделят между служители, изпълнители или други страни, които работят от името на КЗД, независимо от

старшинството или отдела. Ако паролата е забравена, тя трябва да бъде нулирана чрез приложимия метод. ИТ персоналът няма достъп до пароли.
3. Всички софтуерни продукти (включително, но не само, приложения и операционни системи) се актуализират. ИТ служителите на КЗД отговарят за инсталирането на всички актуализации, свързани със сигурността, след като актуализациите се предоставят от издателя или производителя или възможно най-бързо и практически възможно, освен ако няма основателни технически причини да не се направи това.
4. Не може да се инсталира софтуер на нито един компютър или устройство, собственост на КЗД, без предварителното одобрение на председателя на КЗД и директора на съответната дирекция.

Организационни мерки

КЗД гарантира, че са взети следните мерки по отношение на събирането, притежаването и обработката на лични данни:
1. Всички служители, изпълнители или други страни, които работят от името на КЗД, трябва да бъдат напълно запознати, както с техните индивидуални отговорности, така и с отговорностите на Комисията съгласно GDPR и съгласно тази Политика и им се предоставя копие от тази Политика.
2. Само лицата, изпълнителите или други лица, работещи от името на КЗД, които се нуждаят от достъп и ползване на лични данни, за да изпълняват правилно своите задачи, имат достъп до лични данни, съхранявани от КЗД, като следва да бъдат обучени по подходящ начин за това.
3. Всички в КЗД, обработващи лични данни, ще бъдат надлежно контролирани.
4. Всички, работещи от името на КЗД с лични данни, се задължават да полагат грижи, предпазливост и дискретност, когато обсъждат въпроси, свързани с работата, свързани с лични данни, независимо дали на работното място или извън него.
5. Методите за събиране, съхраняване и обработване на лични данни се оценяват и преглеждат редовно.
6. Всички лични данни, съхранявани от КЗД, се преглеждат периодично и изпълнението на обработващите лични данни, трябва редовно да се оценява.
7. Всички обработващи лични данни са длъжни да го направят в съответствие с принципите на GDPR и тази политика.
8. Когато някой, работещ от името на КЗД и обработващ лични данни, не изпълни задълженията си по тази Политика, ще обезщети и ще обезвреди КЗД срещу всякакви разходи, отговорност, вреди, загуби, искове или производства, които могат да възникнат от този неуспех.

Прехвърляне на лични данни в страна извън ЕИП

КЗД може от време на време да прехвърля („прехвърляне" включва предоставяне дистанционно) лични данни на страни извън ЕИП.

Прехвърлянето на лични данни в страна извън ЕИП се извършва само ако се прилагат едно или повече от следните условия:

1. Прехвърлянето е към страна, територия или един или повече специфични сектори в тази страна (или международна организация), за които Европейската комисия е определила, че осигурява адекватно ниво на защита на личните данни;

2. Прехвърлянето е към страна (или международна организация), която осигурява подходящи предпазни мерки под формата на правно обвързващо споразумение между държавните органи или органи; обвързващи корпоративни правила; стандартните клаузи за защита на данните, приети от Европейската комисия; спазването на одобрен от надзорния орган кодекс за поведение (например Службата на комисаря по информацията); сертифициране по одобрен механизъм за сертифициране (както е предвидено в GDPR); договорни клаузи, договорени и разрешени от компетентния надзорен орган; или разпоредби, въведени в административни договорености между публични органи или органи, упълномощени от компетентния надзорен орган;

3. Прехвърлянето се извършва с информирано съгласие на съответния (ите) субект (и) на данните за служителите;

4. Прехвърлянето е необходимо за изпълнението на договор между субекта на данни и КЗД (или за предприсъединителните мерки, предприети по искане на субекта на данни за служителя);

5. Прехвърлянето е необходимо поради важни причини от обществен интерес;

6. Прехвърлянето е необходимо за извършване на съдебни искове;

7. Прехвърлянето е необходимо, за да се защитят жизненоважните интереси на субекта на данни на служителя или на други лица, когато физическото или юридическото лице не е в състояние да даде своето съгласие;

8. Прехвърлянето се извършва от регистър, който според законодателството на Обединеното кралство или ЕС е предназначен да предоставя информация на обществеността и който е отворен за достъп от страна на обществеността като цяло или по друг начин на тези, които са в състояние да демонстрират легитимен интерес достъп до регистъра.

XIII. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

По смисъла на настоящата Политика:

§1. „*Администратор на лични данни*“ е Комисията за защита от дискриминация, като действия от името на администратора осъществява председателят на КЗД.

§2. „*Обработване“* означава 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;

§3. Настоящата Политика е одобрена от председателя на КЗД доц. д-р Ана Джумалиева.

§4. Политиката е в действие от: 25.05.2018 г.