“ИСП.БГ” ООД

ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

ВЕРСИЯ 1/25.05.2018Г.

Утвърдил:.....
/ Александър Семов /

Съдържание

1. Предназначение, обхват и ползватели

2. Референтни документи

3. Дефиниции

4. Основни принципи, отнасящи се до обработката на лични данни
4.1. Законосъобразност, честност и прозрачност
4.2. Ограничение на предназначението
4.3. Минимизиране на данните
4.4. Точност
4.5. Ограничение на сроковете за съхранение
4.6. Почтеност и поверителност
4.7. Отговорност

5. Изграждане на предпазване на данните в бизнес процесите
5.1. Събиране
5.2. Използване, съхранение и премахване
5.3. Оповестяване на трети страни
5.4. Трансграничен трансфер на лични данни
5.5. Право на достъп от субекти на данни
5.6. Преносимост на данни
5.7. Правото на бъдеш забравен

6. Насоки за добросъвестна обработка
6.1. Известия към субектите на данни
6.2. Получаване на съгласие

7. Организация и отговорности
8. Насоки за създаване на водещ надзорен орган
8.1. Необходимост от създаване на водещ надзорен орган
8.2. Основно място на установяване и водещ надзорен орган
8.2.1. Основно място на установяване на администратора на данни
8.2.2. Основно място на установяване на обработващия данни
8.2.3. Основно място на установяване за администратори и обработка данни извън ЕС

9. Действия и отговор на инциденти за нарушаване на личните данни

10. Одит и отговорност

11. Конфликт със закона

12. Управление и съхранение на записи на базата на този документ

13. Валидност и управление на документи

1. Предназначение, обхват и ползватели.

„ИСП.БГ“ ООД , наричана по долу дружество се стреми да спазва приложимите закони и разпоредби, свързани със защитата на личните данни в държавите, в които дружеството оперира. Тази политика определя основните принципи, чрез които компанията обработва личните данни на потребители, клиенти, доставчици, бизнес партньори, служители и други лица, и посочва отговорностите на бизнес отделите и служителите по време на обработката на лични данни.

Тази политика важи дружеството и неговите пряко или непряко контролирани изцяло притежавани дъщерни дружества, които извършват дейност в рамките на Европейско икономическо пространство (ЕИП) или обработват личните данни на субекта на данни в ЕИП. Потребители на този документ са всички служители, постоянни или временни, и всички изпълнители, които работят от името на Организацията.

2. Референтни документи.

- EU GDPR 2016/679 (Регламент ЕС 2016/679 на Европейския парламент и на съвета от 27 април 2016г. За защита на физическите лица при обработването на личните данни и за свободното движение на такива данни и за отмяна на Директива 95/46/ ЕО)
- Съответно национално законодателство или правило за прилагане на GDPR
- Други местни закони и разпоредби
- Политика за защита на личните данни на служителите
- Политика за съхранение на данни
- Описание на длъжността на служителя по защита на данните
- Насоки за опис на данните и обработка на данни
- Процедури за заявка за достъп до физически лица
- Насоки за оценка на въздействието на защита на данните
- Процедура за трансграничен трансфер на личните данни
- Политики за информационна сигурност
- Процедури за уведомяване за нарушение

3. Дефиниции

Следните определения на термините, използвани в този документ, са дефинирани в общия регламент относно защитата на данните на Европейския съюз: „Лични данни“ означава всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни“); физическо лице, което може да бъде идентифицирано, което е лице, което може да бъде идентифицирано, пряко или непряко, по специално чрез идентификатор като име, идентификационен номер, данни за местонахождение, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената икономическата, културната или социалната идентичност на това физическо лице.

Чувствителни лични данни: Личните данни, който по своята същност са особено чувствителни по отношение на основните права и свободи, заслужават специфична защита, тъй като контекстът на тяхната обработка може да създаде значителни рискове за основните права и свободи. Тези лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикати, генетични данни, биометрични данни, с цел еднозначно идентифициране на физическо лице, данни относно здравето или данни, отнасящи се до пола на физическото лице, живот или сексуална ориентация.

Администратор на данни: физическо или юридическо лице, публичен орган, агенция или друга структура, която сама или съвместно с други определя целите и средствата за обработването на личните данни; когато целите и средствата за това обработване се определят от правото на Съюза или правото на държавата членка, администраторът или специалните критерии за неговото определяне могат да бъдат установени в правото на Съюза или в правото на държава членка.

Обработващият данни: физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора.

Обработване: всяка операция или съвкупност от операции, извършени 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.

Псевдонимация: обработване на лични данни по такъв начин, че личните данни не могат повече да бъдат свързани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирано физическо лице или с физическо лице, което може да бъде идентифицирано.

Трансгранично обработване: а) обработване на лични данни, което се осъществява в контекста на дейностите на местата на установяване в повече от една държава членка на администратор или обслужващ лични данни в Съюза, като администраторът или обработващите личните данни е установен в повече от една държава членка; или б) обработване на лични данни , което се осъществява в контекста на дейностите на едно-единствено място на установяване на администратор или обработващия лични данни в Съюза, но което засяга съществено или е вероятно да засегне съществено субекти на данни в повече от една държава членка.

Надзорен орган: независим публичен орган, създаден от държава членка съгласно член 51 на Регламента.

Водещ надзорен орган: надзорният орган, който носи основната отговорност за извършването на трансграничната дейност по обработка на данни. Например когато субекта на данни подаде жалба относно обработката на личните му данни, органът е отговорен, наред с другото за получаване на уведомления за нарушаване на данните, за уведомяване за рискова обработка и има пълна власт по отношение на задълженията си, за да гарантира спазването на разпоредбите на Регламента.

Всеки **„местен надзорен орган“** ще продължи да поддържа на своя собствена територия и ще наблюдава всички местни обработки на данни, които засягат субектите на данни или които се извършват от администратор, или обработващ от ЕС, или извън ЕС, когато обработването им е насочено към субекти на данни, пребиваващи на нейна територия. Техните задачи и правомощия включват провеждане на разследвания и прилагане на административни мерки и глоби, насърчаване на обществена информираност за рисковете , правилата , сигурността и правата във връзка с обработване на лични данни, както и достъпа до помещения на администратора и обработващия, включително оборудване и средства за обработка на данни.

„Основно място на установяване“ означава: а) по отношение на администратор, установен в повече от една държава членка – мястото, където се намира централното му управление в Съюза, освен в случаите когато решенията по отношение на целите и средствата за обработването на личните данни се вземат на друго място на установяване на администратора в Съюза и на това място на установяване има правомощия за прилагане на тези решения, в който случай мястото на установяването, където са взети тези решения, се счита за основно място на установяване; б) по отношение на обработващия лични данни, установен в повечето от една държава членка – мястото, където се намира централното му управление в Съюза, или ако обработващият лични данни няма централно управление в Съюза, мястото на установяване на обработващият лични данни в Съюза, където се осъществяват основните дейности по обработването в контекста на дейностите на дадено място на установяване на обработващия лични данни, доколкото обработващият има специфични задължения съгласно Регламента.

Групово предприятие: контролиращо предприятие и контролираните от него предприятия.

4. Основни принципи, отнасящи се до обработката на лични данни.

Принципите на защита на данните очертават лични данни. В член 5, параграф 2 от EU GDPR се посочва, че „*администраторът е отговорен и е в състояние да докаже спазването на принципите.*“

4.1. Законосъобразност, честност и прозрачност.

Личните данни трябва да бъдат обработвани законосъобразно, справедливо и по прозрачен начин по отношение на субекта на данните.

4.2. Ограничение на предназначението.

Личните данни трябва да се събират за конкретни, изрични и законно съобразни цели и да не се обработват по начин, който е несъвместим с тези цели.

4.3. Минимизиране на данните.

Личните данни трябва да бъдат адекватни, уместни и ограничени до това, което е необходимо по отношение на целите, за които се обработват.

4.4. Точност.

Личните данни трябва да бъдат точни и при необходимост, актуализирани; трябва да се предприемат разумни стъпки, за да се гарантира, че неточните

лични данни, като се имат предвид целите, за които се обработват, се изтриват или коригират своевременно.

4.5. Ограничение за сроковете за съхранение.

Личните данни трябва да се съхраняват не повече от времето, необходимо за целите, за които се обработват личните данни.

4.6. Почтеност и поверителност.

Взимайки предвид състоянието на технологиите и другите налични мерки за сигурност, разходите по внедряването, вероятността и тежестта на рисковете, свързани с личните данни, дружеството трябва да използва подходящи технически или организационни мерки за обработка на личните данни по начин, който гарантира подходяща сигурност на личните данни, включително защита срещу случайно или незаконно унищожаване, загуба, редуване, неразрешен достъп или разкриване.

4.7. Отговорност.

Администраторите на данни трябва да отговорят и да могат да докажат съответствие с принципите, изложени по-горе.

5. Изграждане на Предпазване на данните в бизнес процесите.

За да се докаже съответствие с принципите за защита на данните, организацията трябва да изгради защита на данните в своите бизнес дейности/ процеси.

5.1. Събиране.

Компанията трябва да се стреми да събере възможно най-малко количество лични данни. Ако личните данни се събират от трета страна, управителят трябва да гарантира, че личните данни се събират законно.

5.2. Използване, съхранение и премахване.

Целите, методите, ограничаването на съхранението и периодът на запазване на личните данни трябва да съответства на информацията, съдържаща се в известието за поверителност. Дружеството трябва да поддържа точността, целостта, поверителността и чувствеността на личните данни въз основа на целта на обработката. Трябва да се използват адекватни механизми за защита, предназначени за защита на личните данни, за да се предотврати откраднването или злоупотребата с личните данни, и да се предотврати нарушаването на личните данни. Управителят отговаря за спазването на изискванията, изброени в този раздел.

5.3. Оповестяване на трети страни.

Когато компанията използва услугите на доставчик или бизнес партньор (трета страна) , за да обработва лични данни от негово име, Управителят трябва да гарантира, че този доставчик ще предостави мерки за сигурност, за да защити личните данни, които са адекватни на свързаните с тях рискове. За тази цел трябва да се използва въпросник за съответствие с GDPR за обработващия лични данни.

Дружеството трябва да изисква по договор от доставчика или бизнес партньора да осигури същото ниво на защита на данните. Доставчикът или бизнес партньора трябва да обработва само лични данни, необходими му за да изпълнява своите договорни задължения към Дружеството или по нареждане на Дружеството, а не за други цели. Когато Дружеството обработва лични данни съвместно с независима трета страна, Дружеството трябва изрично да уточни своите съответни отговорности и третата страна в съответния договор или друг правно обвързващ документ, като например Споразумението за обработка на данни от доставчиците.

5.4. Трансграничен трансфер на лични данни.

Преди да се предадат личните данни извън Европейското икономическо пространство (ЕИП), трябва да се използват адекватни предпазни мерки, включително подписването на споразумение за прехвърляне на данни, както се изисква от Европейския съюз, и при необходимост трябва да бъде получено разрешение от съответния орган за защита на данните. Предприятието, което получава личните данни, трябва да спазва принципите за обработка на лични данни, посочени в процедурата за трансгранично предаване на данни.

5.5. Право на достъп от субекти на данни.

Когато действа като администратор на данни, управителят е отговорен да предоставя на субектите на данни механизъм, който им позволява да имат разумен достъп до личните си данни, и трябва да им позволява да актуализират, коригират, изтриват или предават своите лични данни, ако е приложимо или се изисква по закон. Механизмът за достъп ще бъде допълнително описан в процедурата за заявка за достъп до субекта на данни.

5.6. Преносимост на данни.

Субектите на данни имат право да получат при поискване копие от данните, които са ни предоставили в структуриран формат, и да предадат тези данни на друг администратор безплатно. Управителят е отговорен да гарантира, че тези искания се обработват в рамките на един месец, не са прекомерни и не засягат правата на лични данни на други лица.

5.7. Правото да бъдеш „забравен“.

При поискване, субектите на данни имат право да получат от дружеството изтриването на личните им данни. Когато Дружеството действа като Администратор на данни, Управителят трябва да предприеме необходимите действия (включително технически мерки), за да информира третите лица, които използват или обработват тези данни (обработващият данни), да се съобразява с искането.

6. Насоки за добросъвестна обработка.

Личните данни трябва да се обработват само при изрично разрешение от Управителя. Компанията трябва да реши дали да извърши оценката на въздействието върху защитата на данните за всяка дейност по обработка на данни, съгласно насоките за оценка на въздействието върху защитата на данните.

6.1. Известия към субектите на данни.

По време на събирането на лични данни за всякакъв вид обработка, включително, но не само, продажба на продукти, услуги или маркетингови дейности, Управителят е отговорен да информира надлежно субектите на данни за следното: видовете лични данни, целите на обработка, методите за обработка, правата на субектите, на данни по отношение на техните лични данни, периода на запазване, потенциалните международни трансфери на данни, ако данните се споделят с трети страни и мерките за сигурност на дружеството за защита на личните данни. Тази информация се предоставя чрез Известие за поверителност.

Когато се споделят лични данни с трета страна, Управителят трябва да гарантира, че субектите на данни са били уведомени за това чрез Известие за поверителност.

Когато се прехвърлят лични данни на трета държава, в съответствие с трансграничната политика за прехвърляне на данни, съобщението за поверителност трябва да отразява това и ясно да посочва къде и кои лични данни се прехвърлят.

Когато се събират чувствителни лични данни, Управителят трябва да се увери, че известието за поверителност изрично посочва целта, за която се събират тези чувствителни лични данни.

6.2. Получаване на съгласие.

Когато обработването на лични данни се основава на съгласие на субекта на данните или на други законови основания, Управителят е отговорен за

запазването на такова съгласие. Управител отговаря за предоставянето на съгласието на субектите на данни, които трябва да дадат съгласие си, и трябва да информира, и да гарантира, че тяхното съгласие (когато съгласието се използва като законно основание за обработка) може да бъде оттеглено по всяко време.

Когато събирането на лични данни в свързано с дете на възраст под 16 години, Управителят трябва да гарантира, че родителското съгласие е дадено преди събирането на, като се използва формулярът за съгласие от родител.

Когато се изисква да се коригират, изменят или унищожат записите с лични данни, Управителя трябва да гарантира, че тези изисквания се обработват в разумен срок. Управителят също трябва да записва заявките и да води дневник за тях.

Личните данни трябва да се обработват само за целите, за които първоначално са били събрани. В случай, че Дружеството иска да обработва събраните лични данни за друга цел, дружеството трябва да потърси съгласието на своите субекти на данни в ясен и кратък срок. Всяко такова искане трябва да включва първоначална цел, за която са събрани данните, както и новата или допълнителна/допълнителните цел/цели. Искането трябва да включва и причината за промяна на целта /целите. Служителят по защита на данните отговаря за спазването на правилата в този параграф.

Сега и в бъдеще, Управителят трябва да гарантира, че методите за събиране са в съответствие със съответните закони, добри практики и индустриални стандарти.

Управителя е отговорен за създаването и поддържането на регистър на известията за поверителност.

7. Организация и отговорности.

Отговорността за осигуряване на подходяща обработка на лични данни се носи от всеки, който работи за или с Дружеството и има достъп до обработваните от компанията лични данни.

Основните отговорности при обработването на лични данни са следните организационни роли и длъжности: Съветът на директорите или друг еквивалентен орган взема решения и одобрява общите стратегии на компанията за защита на личните данни.

Служителят по ***Защита на личните данни (ДЗД) или друг служител, отговорен*** за управлението на програмата за защита на личните данни и отговарящ за разработването и популяризирането на политика за защита на личните данни, както е определено в описанието на длъжностната характеристика на служителя за защита на данните;
Юридическият отдел заедно със Служителя по защита на данните наблюдава и анализира законите за лични данни и промените в нормативната уредба, разработва изисквания за съответствие и помага бизнеса в постигането на целите си за лични данни.

DPO (Data Protection Officer) е отговорен за:

- Осигуряване на всички системи, услуги и оборудване, използвани за съхранение на данни, да отговарят на приемливи стандарти за сигурност.
- Извършване на редовни проверки и сканиране, за да се гарантира, че хардуерът и софтуерът за сигурност функционират правилно.
- Одобряване на всички декларации за защита на данните, прикрепени към съобщения, имейли и писма.
- Отговори на всякакви запитвания за защита на данните от журналисти или медии.
- Когато е необходимо, работи със служителя по защита на данните, за да се гарантира, че маркетинговите инициативи спазват принципите на защита на данните.
- Подобряване на информираността на служителите относно защитата на лични данни на потребителите.
- Организиране на експертни познания за защита на личните данни и обучение за повишаване на информираността на служителите, работещи с лични данни.
- Защита на личните данни на служителите от „край до край“. Това трябва да гарантира, че личните данни на служителите се обработват въз основа на законовите бизнес цели и необходимост а работодателя.
- Да отговаря за предаването на отговорностите за защита на личните данни на доставчиците и за повишаване на нивата на информираност на доставчиците за защита на личните данни, както и за понижаване на изискванията за лични данни към трети страни, които използват. Отделът за поръчки/ доставки трябва да гарантира, че Дружеството си запазва правото да извършва одит на доставчици.

8. Насоки за създаване на Водещ надзорен орган.

8.1. Необходимост от създаване на Водещ надзорен орган.

Определянето на водещ надзорен орган е уместно само ако Дружеството извършва трансгранично обработване на лични данни.

Трансгранично обработване на лични данни е извършено, ако:

а) *Обработването на лични данни се извършва от дъщерни дружества на Дружеството, което се намира в други държави – членки;*

или

б) *Обработката на лични данни, която се извършва в едно предприятие на Дружеството в ЕС, съществено засяга или има вероятност да засегне съществено субектите на данни в повече от една държава-членка*.

Ако Дружеството има учреждения само в една държава членка и неговите обработвани данни засягат само субекти на данни в тази държава- членка, то няма нужда да се създаде водещ надзорен орган. Единственият компетентен орган ще бъде надзорният орган в страната, в която Дружеството е законно учредено.

8.2. Основно място на установяване и водещ надзорен орган.

8.2.1. Основно място на установяване и водещ надзорен орган. Висшето ръководство на дружеството трябва да идентифицира основното си място на установяване, така че да може да се определи водещият надзорен орган. Ако дружеството е със седалище в държава-членка на ЕС и вземе решения, свързани с трансгранични преработващи дейности на мястото на централната му администрация, ще има единствен водещ надзорен орган за дейностите по обработка на данните, извършени от дружеството. Ако дружеството има множество предприятия, които действат самостоятелно и вземат решения относно целите и средствата за обработка на лични данни, Висшето ръководство на дружеството трябва да приеме, че съществуват повече от един водещ надзорен орган.

8.2.2. Основно място на установяване на обработващия данни. Когато Дружеството действа като Обработващ данни, основното

предприятие ще бъде мястото на централната администрация. В случай, че мястото на централната администрация не се намира в ЕС, основното предприятие ще бъде учредено в ЕС, където се извършват основните дейности по обработване.

8.2.3. Основно място на установяване за администратори и обработващи данни извън ЕС.

Ако дружеството няма основното предприятие в ЕС, а има дъщерни дружества в ЕС, тогава компетентният надзорен орган е местният надзорен орган.
Ако Дружеството няма основно предприятие в ЕС, нито дъщерните дружества в ЕС, то трябва да назначи свой представител в ЕС, а компетентният надзорен орган ще бъде местен надзорен орган, в който се намира представителят.

9. Действия в отговор на инциденти за нарушаване на личните данни.

Когато организацията узнае за предполагаемо или действително нарушение на личните данни, Управителят трябва да извърши вътрешно разследване и своевременно да предприеме подходящи мерки за отстраняване, в съответствие с политиката за нарушаване на данните. Когато Съществува риск за правата и свободите на субектите на данни, Дружеството трябва да уведоми съответните органи за защита на данните без неоснователно забавяне и, когато е възможно – в рамките на 72 часа.

10. Одит и отговорност.

Отделът за одит или друг оторизационен отдел отговаря за проверката/одита на това, колко добре бизнес отделите прилагат тази политика.
Всеки служител, който нарушава тази Политика, ще бъде обект на дисциплинарно действие и служителят може също да бъде обвързан с граждански или наказателни задължения, ако неговото поведение нарушава закона или подзаконови актове.

11. Конфликт със Закона.

Тази политика е предназначена да спазва законите и подзаконовите актове на мястото на установяване и на страните, в които Организацията работи. В случай на конфликт между тази политика и приложимите закони и разпоредби, последните имат предимство.

12. Управление и съхранение на записи на база на този документ.

Име на записа	Място на съхранение	Отговорник за съхранението	Контроли за защита на записите	Време за съхранение
Формуляри за съгласие на субекти на данни	Интранет	Управител	Само упълномощени служители имат достъп по формулярите	10 години
Формуляр за отказ от съгласие на субекта на данните	Интранет	Управител	Само упълномощени служители имат достъп по формулярите	10 години
Регистър на съобщенията за поверителност	Интранет	Управител	Само упълномощени служители имат достъп по формулярите	Постоянно

13. Валидност и управление на документи.

Този документ е валиден от 25.05.2018 г.

Собственикът на този документ е Управителят той трябва да провери и ако е необходимо да актуализира документа най-малко веднъж годишно.

Управител:

/Александър Семов /