НУПРОВИА ЕООД

ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Код:	01.1
Версия:	1.0
Дата на версията:	21.08.2019 г.
Създаден от:	Стефан Иванов
Одобрен от:	Огнян Иванов
Ниво на конфиденциалност:	Некласифициран

Хронология на промяната:

Дата	Версия	Създаден от	Описание на промяната
21.08.2019	1.0	НУПРОВИА ЕООД	Основен документ - създаване

Съдържание

1. Цел, обхват и потребители

НУПРОВИА ЕООД, наричано още „Дружеството“, полага усилия за съответствие и съобразяване с Общия регламент относно защита на данните 2016/697 на ЕС и националното законодателство в областта на защита на личните данни.

Настоящата политика определя общите принципи, изисквания и отговорности, съгласно които се осъществява събирането и обработването на лични данни в Дружеството. Тя е основа за разработване и внедряване на система за защита на личните данни и доказване на съответствието с регламентиращите документи.

Политиката цели също така да информира служителите, партньорите, контрагентите и институциите за ангажиментите на Дружеството за опазване на личните данни.

Политиката се отнася за всички служители на Дружеството и Субектите, чиито лични данни се обработват.

Потребители на документа са всички служители на Дружеството, в т.ч. временно заетите и стажантите.

2. Регламентиращи и свързани документи

- EU GDPR 2016/679 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC)
- Закон за защита на личните данни
- Закон за защита на класифицираната информация
- Търговски закон
- Закон за счетоводството
- Кодекс на труда
- Закон за здравето
- Закон за здравословните и безопасни условия на труд
- Политики и процедури от системата за защита на личните данни

3. Определения

В настоящия документ се използват следните определения на термините, произтичащи от чл. 4 на Регламента:

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, 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 социална идентичност на това физическо лице;

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

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

Обработващ лични данни: означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на администратора;

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;

Анонимизация: Необратима де идентификация на личните данни, така, че лицето не може да бъде разпознато без заделяне на значителни ресурси, технологии и време. Тези данни повече не се разглеждат като лични данни и принципите за обработка на лични данни не се прилагат спрямо тях.

Псевдонимизация: означава обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани 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;

Трансгранична обработка на лични данни: Предаване на лични данни, които се обработват или са предназначени за обработване след предаването на трета държава или на международна организация, се осъществява само при условие че са спазени другите разпоредби на настоящия регламент, само ако администраторът и обработващият лични данни спазват условията по настоящата глава, включително във връзка с последващи предавания на лични данни от третата държава или от международната организация на друга трета държава или на друга международна организация.

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

4. Основни принципи, свързани с обработването на личните данни.

Принципите за защита на личните данни определят основните отговорности на организациите, обработващи лични данни. Съгласно чл. 5 (2) Администраторът на лични данни е отговорен и длъжен да може да докаже тяхното спазване . Регламентът определя следните принципи:

4.1. Законосъобразност, добросъвестност и прозрачност

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

4.2. Ограничение на целите

Лични данни, събирани за конкретни, изрично указани и легитимни цели, не се обработват по-нататък по начин, несъвместим с тези цели;.

4.3. Свеждане на данните до минимум

Личните данни трябва да са подходящи, свързани с и ограничени до необходимото във връзка с целите, за които се обработват. Дружеството следва да прилага мерки за анонимизация и псевдонимизация, където е приложимо, за да намали риска за тези данни.

4.4. Точност

Личните данни трябва да бъдат точни и при необходимост да бъдат поддържани в актуален вид. Трябва да се предприемат всички разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват.

4.5. Ограничение на съхранението

Личните данни следва да се съхраняват за период, предвиден от закона и не по-дълъг от необходимото за целите, за които се обработват личните данни;

Личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели;

4.6. Цялостност и поверителност

Личните данни следва да се обработват по начин, който гарантира подходящо ниво на сигурност на личните данни, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки.

4.7. Отчетност

Администраторът на лични данни е отговорен за спазването на принципите и да е в състояние да докаже, че обработката на лични данни се извършва съобразно тях.

5. Защита на данните на етапа на проектирането и по подразбиране във всички бизнес процеси, осъществявани от Дружеството.

При въвеждане на система са защита на личните данни и за доказване на съответствието на прилагането й с принципите за защита на данните се залага прилагане на организационни и техническите мерки и средства във всички бизнес процеси, осъществявани в момента или предвидени за използване в бъдеще. Системата трябва да позволява съвместимост с въвеждани електронни информационни системи.

5.1. Уведомяване на Субектите на данни

Субектите на лични данни се уведомяват преди събирането и обработката на техните данни. Редът за уведомяване е посочен в т. 6.1. на настоящата политика.

5.2. Право на избор и съгласие от страна на Субектите на данни

В случаите, когато личните данни се събират въз основа на съгласие, Субектите на данни имат право на избор и заявяване на изричното си съгласие, както и на неговото оттегляне. Редът за това е посочен в т. 6.2 на настоящата политика.

5.3. Събиране на лични данни

В Дружеството се събират само изискваните от закона лични данни, необходими и достатъчни за целите на обработка и осъществяване дейността му.

В НУПРОВИЯ ЕООД се получават лични данни от контрагентите, клиенти, доставчици и партньори на Дружеството.

5.4. Използване, Съхранение и Унищожаване

Редът за използване, съхранение и унищожаване на лични данни е регламентиран в отделна политика и процедура, определящи условията на съхранение и използване, сроковете за съхранение и методите на унищожаване. Чрез тях се гарантира целостта, точността и наличността на данните, като се осигурява надеждната им защита от пробив, манипулиране, унищожаване или откradване.

5.5. Разкриване на информация пред трети страни

НУПРОВИА ЕООД има задължение да разкрива информация за лични данни в следните случаи:

- Пред държавни институции на основание на законови изисквания;
- При провеждане на национални или международни разследвания по искане на надзорните органи.

Нупровиа ЕООД може да предоставя документи, съдържащи лични данни, на трети лица в качеството им на доставчици на услуги.

5.6. Трансфер на лични данни в трети държави

НУПРОВИА ЕООД не осъществява трансфер на лични данни в трети страни извън Европейското икономическо пространство. В случай, че това се наложи в бъдеще това ще става след получаване на изрично разрешение от Държавната комисия за защита на личните данни при спазване на процедурите за проверка на съответствието на получаващата страна. Дейността по трансфера на данни е описана в отделна Процедура.

5.7. Право на достъп до информация на Субектите на данни

В качеството си на Администратор на лични данни НУПРОВИА ЕООД поема отговорност за осигуряване безплатно на достъп до лични данни на Субекта на данни в срок до 30 дни от заявеното искане. Предоставянето на информация става съгласно процедура след писмено заявление по образец.

5.8. Преносимост на данните

Субектите на данни имат право на пренос на данните като по тяхно искане получат копие от данните, които са предоставили, в структуриран формат и да поискат прехвърляне на тези данни към друг Администратор. Това право не е безусловно и зависи от техническата възможност, необходимите усилия и време, което не отменя задължението Субектът на данни да бъде информиран за решението на Администратора в предвидения срок от 30 дни.

5.9. Право на изтриване (право да бъдеш забравен)

НУПРОВИА ЕООД се задължава до осигури изтриване на личните данни на Субекти на данни по тяхно искане, а когато става дума за деца по искане на техните родители или настойници по установената форма и процедура. При наличие на законови основания личните данни да не се изтриват, субектът на данни се уведомява в срок от 30 дни.

6. Указания за справедлива обработка на личните данни.

Дружеството осъществява анализ за риска и въздействието върху субектите на данни и взема решение дали е необходимо да извърши Оценка на въздействието на защитата на данните, съгласно Указанията и Методиката за извършване на такава оценка.

6.1. Уведомления до Субектите на данни

Преди и при събиране на лични данни и обработка от какъвто и да е тип, Дружеството има отговорност ясно да информира субектите на данни относно:

- Типа и вида на личните данни, които се събират;
- Целите, за които се събират и обработват;
- Методите на обработка на личните данни;
- Срока на съхранение на данните;
- Правата на субектите на данни;
- Възможен трансфер на данни в трети страни;

- Пред кого могат да бъдат разкривани личните данни;
- Какви мерки за защитата на данните се предприемат.

НУПРОВИА ЕООД прилага селективен подход при информиране на Субектите на данни чрез различен формат на Уведомления за поверителност, насочени към различните категории лица.

В случай, че се налага събиране на чувствителни лични данни, ДЛЗД трябва да вземе мерки лицата да бъдат уведомени за целите на събиране и обработка с изрично уведомление или формуляр за съгласие.

6.2. Получаване на съгласие

Когато личните данни се обработват въз основа на съгласие на субектите на данни, Субектите на лични данни трябва надлежно да бъдат уведомени за условията на съгласието им и правото им да го оттеглят по всяко време.

Когато се събират лични данни за деца под 16 години ДЛЗД трябва да осигури получаването на родителско съгласие преди започване на обработката на данните. Това става с Формуляр за родителско съгласие.

Когато има искане за коригиране, допълване или унищожаване на лични данни, ДЛЗД трябва да осигури всички заявки да бъдат обработени в регламентирания срок и да води дневник за постъпилите заявки.

Личните данни следва да се обработват само за целта, за която първоначално са събирани. В случай, че Дружеството желае да обработва лични данни за друга цел, то трябва да поиска и получи съгласие от Субектите на данни. Искането на съгласие трябва да съдържа оригиналната цел за събиране на данните и новите или допълнителни цели, както и причините за промяна на целите.

Управителят на Дружеството трябва да осигури методите за събиране и обработка на лични данни да бъдат в съответствие с действащото законодателство, стандарти и добри практики.

Той отговаря за създаването и поддържането в актуално състояние Уведомленията за поверителност и списъка с уведомления.

7. Организация и отговорности по защитата на личните данни

НУПРОВИА ЕООД носи отговорност за съответствието с Общия регламент и за нарушения на личните данни в качеството му на Администратор и Обработващ на лични данни.

Всеки отделен служител носи персонална отговорност в рамките на функционалните си задължения по защита на личните данни.

Управителят определя общата стратегия, отговаря за защитата на личните данни, взема решения, одобрява политики, процедури и документи и следи за прилагането на системата.

8. Надзорен орган

Надзорен орган, съгласно изискванията на чл. 51 от Общия регламент относно защитата на личните данни и Закона за защита на личните данни, е Комисията за защита на личните данни.

9. Уведомяване на надзорния орган за нарушение на сигурността на личните данни

При установяване на нарушение на сигурността на личните данни Управителят извършва вътрешно разследване и взема незабавни мерки за установявана характера, обема и риска от нарушението или инцидента. В случай на установяване на риск за правата и свободите на Субектите на данни Дружеството уведомява надзорния орган в рамките на 72 часа. Дружеството също така уведомява и Субектите на данни, засегнати от нарушението или инцидента.

10. Проверки и отчетност

Веднъж годишно се извършва цялостен преглед на системата за защита на личните данни под ръководството на Управителя. След анализ на резултатите от прегледа, при необходимост Политиката за защита на личните данни се обновява.

Всеки служител, обработващ лични данни носи отговорност за спазване на политиките, процедурите и документите по защита на личните данни и подлежи на административна отговорност за допуснати нарушения. При установяване на умишлена злоупотреба и престъпно използване на лични данни лицата носят и наказателна отговорност.

11. Управление на документите, свързани с настоящата политика

Документ	Място на съхранение	Отговорник	Контрол	Срок на съхранение
Политика за защита на личните данни на служителите	Папка GDPR на служебен компютър	ДЛЗД	Управител	Безсрочно
Политика по съхранение на данните	Папка GDPR на служебен компютър	ДЛЗД	Управител	Безсрочно
Политика за информационна сигурност	Папка GDPR на служебен компютър	ДЛЗД	Управител	Безсрочно
Политика за обучение по общия регламент относно защитата на данните (ОРЗД)	Папка GDPR на служебен компютър	ДЛЗД	Управител	Безсрочно
Уведомления	Папка GDPR на служебен компютър	ДЛЗД	Управител	Безсрочно
Съгласия	Папка GDPR на служебен компютър	ДЛЗД	Управител	Безсрочно
Процедури	Папка GDPR на служебен компютър	ДЛЗД	Управител	Безсрочно
Въпросници	Папка GDPR на служебен компютър	ДЛЗД	Управител	Безсрочно
Формуляри	Папка GDPR на служебен компютър	ДЛЗД	Управител	Безсрочно

12. Валидност и управление на документа.

Настоящият документ влиза в сила от 21.08.2019 г.

Администратор на настоящия документ е Управителят.

УПРАВИТЕЛ НА НУПРОВИА ЕООД
ОГНЯН ИВАНОВ