Технически и организационни мерки за защита на личните данни

Общи правила

Настоящите правила уреждат техническите и организационни мерки за защита на личните данни в **ИНОВАТИВНО ДПК**, ЕИК **208533828**, в изпълнение на изискванията на чл. 24 (1) от Регламент 2016/679 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните).

Приетите техническите и организационни мерки за защита на личните данни целят създаване на процеси при обработването на личните данни и управление на риска при обработването на тези данни.

Организационните и техническите мерки за защита на личните данни се състоят от мерки за:

1. КОНФИДЕНЦИАЛНОСТ НА ДАННИТЕ
2. ЗАПАЗВАНЕ НА ЦЕЛОСТТА И ТОЧНОСТТА НА ДАННИТЕ
3. СЛУЧАЙНА ЗАГУБА И ЗАЩИТА ПРИ ПРОБИВ
4. МЕРКИ ЗА ЗАЩИТА НА ДАННИТЕ ПРИ ПРЕДАВАНЕ, ПРЕХВЪРЛЯНЕ И ВЪЗЛАГАНЕ
5. ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

ИНОВАТИВНО ДПК
СОФИЯ,
БЪЛГАРИЯ
INNOVATIVE DPK

КОНФИДЕНЦИАЛНОСТ НА ДАННИТЕ

Настоящите технически и организационни мерки уреждат запазването на конфиденциалността на данните, като вземат предвид текущото положение на технологиите, стойността на необходимите разноски за привеждане на описаните мерки в действие и естеството, обхвата и контекста и целите на обработката на лични данни, както и рисковете, които биха могли да възникнат за правата и свободите на субектите на данните.

Мерки за контрол на достъпа

Дружеството приема следните мерки за контролиране и ограничаване на достъпа до своята физическа и дигитална инфраструктура.

Физически мерки

- Физическият достъп до работните пространства е ограничен.
- В работните помещения е инсталирана алармена система и същите се охраняват от охранителна фирма.
- Всички външни лица задължително се посрещат от служител и се записват.
- Личните данни на хартиен носител се съхраняват в заключващи се шкафове, като предаването на ключове за шкафовете се документира. Ключове се предават единствено на оправомощените лица.

Дигитален достъп

- Въведени са правила и задължителни изисквания към паролите за достъп до работните системи като минимална дължина, задължително периодично изменение, задължително съдържание на символи и/или цифри.
- Достъпът до системите се блокира автоматично след няколко неуспешни опита за вход.
- Споделянето на пароли е стриктно забранено. Всички пароли се съхраняват в криптирана форма. Всяко работно устройство се използва с парола, която е задължителна за въвеждане след неактивност на устройството.
- Управлението на паролите в организацията се осигурява чрез специализиран софтуер.

- За критични системи, сигурността на достъпа се обезпечава чрез допълнителни мерки за сигурност на входа като двустепенна верификация (2FA).

Организационен достъп

- Всеки служител или трето лице с достъп до лични данни в работните ни системи ни има индивидуален профил с ограничен достъп. Достъпът до данните е минимизиран само до тези, които са необходими, за изпълнението на служебните задължения.
- Всяко лице, нает от Дружеството има определена роля с ясно зададени правомощия за обработка на личните данни.
- Дружеството прилага политика за „Clean Desk Policy“, съгласно която служителите са длъжни да не оставят документи, носители на информация или устройства, съдържащи лични данни, без надзор на работните си места.
- Дружеството използва администраторски инструменти, чрез които надзирава и контролира обработването на личните данни .
- Дружеството поддържа минимален брой администраторски профили.
- Достъпът до данните се предоставя на базата на необходимостта данните да бъдат обработвани.
- Личните данни са класифицирани в зависимост от тяхната чувствителност.
- Работните устройства и мрежи и устройства са защитени от неправомерен достъп чрез Firewall.
- Достъпът до работните сървъри е стриктно ограничен и могат да бъдат използвани единствено от предварително определени IP адреси (white list)

Разделяне на данните според целите

Разделението на личните данни според целите, за които се обработват, се осигурява чрез създаване на дейности по обработване на лични данни преди да започне самото обработване.

ЗАПАЗВАНЕ НА ЦЕЛОСТТА И ТОЧНОСТТА НА ДАННИТЕ

Дружеството създава мерки за гарантиране на пълнотата и точността на обработваните лични данни и осигурява защита срещу неправомерни промени в обработваните лични данни.

ИНОВАТИВНО ДПК
СОФИЯ, БЪЛГАРИЯ
INNOVATIVE DPK

- Първоначалното записване и последващите промени в личните данни се документират, като се дава възможност да се разбере кой, кога и как е въвел или изменил данните.
- Въведени са периодични задължителни обновления на работните системи, осигуряващи сигурността.

Защита на работните устройства

Дружеството е приело следните правила относно защитата на работните устройства:

- На работните устройства могат свободно да се свалят файлове, доколкото няма изрична забрана.
- На работните устройства може свободно да се достъпват всички уебсайтове, доколкото няма изрична забрана.
- На работните устройства не могат свободно да се инсталират приложения, доколкото няма изрично разрешение за конкретното приложение. Всички приложения трябва да бъдат изтегляни единствено от сигурни източници (например, сайта на производителя)
- Работните имейли са защитени с anti-spam филтър, който блокира съмнителните съобщения. Всички служители са обучени относно често срещаните фишинг и други атаки и са инструктирани при съмнение да не отварят потенциално опасни имейли и незабавно да се свържат със системния администратор.
- Извън стандартните мерки за сигурност служителите, работещи дистанционно, са задължени да криптират своите твърди дискове с актуални криптографски методи като например Apple FileVault или друг аналогичен.
- Периодично се извършват тестове на сигурността на работните системи, които се документират.
- В лог-файлове се записва информация относно извършените действия в работните системи от потребителите.

СЛУЧАЙНА ЗАГУБА И ЗАЩИТА ПРИ ПРОБИВИ

Полагаме всички усилия да ограничим неправомерния достъп до данните, както и да ги защитим от случайна загуба. Въпреки това, не е възможно да бъде изцяло гарантирана сигурността на данните, поради което сме приели следните мерки за защита при

случайното увреждане или унищожаване на личните данни и за ограничаване на въздействието при пробив и неправомерен достъп до данните:

- На всеки 24 часа се прави автоматично резервно копие (backup) на цялата информация от работните системи. Автоматичните резервни копия се съхраняват за период от една седмица.
- При разработване на нови функционалности се прави ръчно резервно копие (backup) на цялата информация от работните системи. Ръчните резервни копия се съхраняват за период от три месеца.
- Хартиените документите, съдържащи лични данни, се сканират и се съхраняват в дигитална форма.
- Данни в покой се съхраняват на криптирани твърди дискове, които не позволяват тяхното възпроизвеждане без необходимия криптографски ключ.
- Данните в движение се криптират като се използват актуалните сертификати и протоколи за сигурност.
- Всички криптографски ключове за декриптиране на информацията се съхраняват по сигурен начин и могат да бъдат достъпени само от оправомощените лица.
- При опасност за сигурността на данните, като например при загуба на работно устройство или кражба, информацията на устройството може да бъде изтрита изцяло дистанционно от системен администратор.
- Регулярно актуализираме практиките си за криптиране на данни, за да осигурим максимална защита на данните и съответствие със законовите изисквания.

Идентифициране на потенциални пробиви в сигурността

В случай на пробив в сигурността на личните данни, или подозрение за такъв пробив, или нещо необичайно, свързано с личните данни, служителят забелязал конкретната нередност, или проявил съмнение за такава, незабавно уведомява Отговорното лице по обработване на личните данни. Незабавно се извършва оценка дали има нарушение на сигурността и се взема решение относно необходимите действия съгласно Общия Регламента за Защита на Данните и вътрешните правила на Дружеството.

Срокове за съхранение на данните

Всяка отделна категория лични данни има собствен период за съхранение, който се определя в правилата относно дейността по обработване на личните данни. Личните

данни се обработват за периода, за който това е необходимо и в съответствие с целите, за които са събрани.

Когато това е необходимо, устройствата, съхраняващи лични данни, се унищожават по надлежен начин, непозволяващ повторното възпроизвеждане на съхраняваната информация. При унищожаването може да се използва услугите на трето лице, което по занятие извършва такова унищожаване и отговаря на необходимите изисквания за сигурност. Хартиени документи, съдържащи лични данни, се унищожават чрез шредер.

МЕРКИ ЗА ЗАЩИТА НА ДАННИТЕ ПРИ ПРЕДАВАНЕ, ПРЕХВЪРЛЯНЕ И ВЪЗЛАГАНЕ

Приложенията и доставчиците на услуги, като например доставчици на облачни услуги, трябва да бъдат одобрени преди тяхната употреба, за да се гарантира съответствие с изискванията за управление на качеството и поверителност на данните.

Използваме само доставчици на услуги трети страни, които са гарантирали съответствието си с приложимите разпоредби за поверителност и други приложими разпоредби. Преди да се ангажираме с доставчик на услуги, ние извършваме надлежна проверка и разглеждаме интегритета, местоположението, историята и предоставената документация на компанията, като политика за поверителност, стандартни договорни клаузи, технически и организационни мерки, споразумения за обработка на данни и др.

Когато е приложимо, подписваме споразумения за защита на данните, включително клаузи за изтриване, ограничаване на обработката на данни и предоставяне на помощ от подизпълнители.

Оправомощен да определя третите лица, с които могат да се споделят лични данни е Отговорникът за дейността по обработване

ОРГАНИЗАЦИОННИ МЕРКИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Съдействие на Администратори и Обработващи данни

Дружеството, в ролята си Обработващ лични данни, оказва необходимото съдействие на Администратора на лични данни и когато е приложимо на друг Обработващ лични данни, включително съдействие при ангажирани други Обработващи подизпълнители.

Администраторът на личните данни може самостоятелно да въвежда, изтрива редактира и експортира данни в работните системи на Дружеството.

При получаване на искане за упражняване на права от субекти на данните, като например изтриване, корекция или др., незабавно пренасочваме искането към Администратора, който е отговорен да окаже необходимото съдействие на субекта на данните. Уведомяваме субекта на данните за извършеното пренасочване.

При необходимост от извършване на оценка на въздействието върху правата и свободите на субектите на данните оказваме съдействие на Администратора.

При нужда от съдействие заинтересованите лице могат да се свържат с контактния център на Дружеството.

Отговорни лица

Вътрешно отговорно лице за спазването на приложимите към Дружеството регулации в областта на личните данни, както и на приетата вътрешна документация е Ирена Иванова. Вътрешно отговорното лице се грижи за оперативните въпроси и периодично извършва отчет на дейността си към ръководството. Имейл за контакт с вътрешно отговорното лице е gdpr@legal-tech.bg.

Класификация на информацията

Използваме следната класификация на информацията:

Информация за служебно ползване	Вътрешната информация е достъпна за служителите на Дружеството и не може да бъде разпространявана извън него.
Поверителна информация	Цялата налична информация, до която служителите имат достъп, е конфиденциална, освен ако изрично не е посочено друго. Информацията може да се използва единствено с цел изпълнение на професионалните задължения на служителите. Всяка информация, която не е изрично класифицирана, се счита за конфиденциална.
Публична информация	Публичната информация е общодостъпна до всички и може да бъде споделяна свободно.
Секретна информация	Строго ограничената информация е достъпна единствено за конкретни служители или роли. Достъпът до тази информация е ограничен както физически, така и дигитално. Информацията, която е класифицирана като строго ограничена, не може да бъде споделяна, освен ако изрично не е предвидено друго.

Отношения с работниците и служителите

Всеки работник или служител на Дружеството при постъпването си на работа се запознава с цялата приложима към него документация по защита на личните данни и се задължава да я спазва, включително но не само разпределената му роля, правилата за дейностите по обработване на лични данни, до които има достъп, настоящите Технически и организационни мерки и др.

Обучения

Работниците и служителите при постъпването си на работа се обучават относно правилата за обработване на личните данни в Дружеството посредством:

- персонални инструктажи и обучения
- групови обучения

Дружеството периодично организира нови обучения за работниците и служителите, които вече са преминали през първоначалното обучение.

Проверка и оценка на актуалността на мерките

Дружеството следва процедура по проверка и оценка на актуалността на мерките за защита на личните данни като периодично, но на не по-дълъг период от 12 месеца, проверява дали съществуващите процеси отговарят на изискванията на privacy by design.

Контакт при запитвания, свързани със защитата на личните данни

Субектите на данните, включително нашите служители, могат да упражняват правата си за защита на личните данни, включително но не само да получават информация за обработваните лични данни, да ограничават обработката, да искат изтриване или поправка и други, като изпратят имейл съобщение до Дружеството. Конкретните данни за контакт и отговорното лице да отговори са посочени в правилата относно приложимата дейност по обработване на лични данни.

Управител: _____
Ирена ИВАНОВА

ИНОВАТИВНО ДПК
СОФИЯ, БЪЛГАРИЯ
INNOVATIVE DPK