Вътрешни правила за защита на данните
в „Съобщително строителство и възстановяване“ ЕАД

Тази вътрешни правила за защита на данните представят принципите и правните условия, които организацията трябва да спази, когато получава, обработва, предава или съхранява лични данни за целите на своята дейност, включително лични данни на клиенти, доставчици и работници или служители. Правилата са в съответствие с изискванията на Общия Регламент за Защита на Данните (Регламент 2016/679) (GDPR).

1. ИНТЕРПРЕТАЦИЯ

1.1.ДЕФИНИЦИИ

Автоматизирано Вземане на Решения: когато дадено решение е взето изцяло на базата на Автоматизирано Обработване (включително профилиране), което води до правни последици или засяга значително физическото лице. GDPR забранява Автоматизираното Вземане на Решения (освен ако определени условия са на лице), но не и Автоматизираното Обработване.

Автоматизирано Обработване: всяка форма на автоматизирано обработване на Лични Данни, състоящо се в употребата на Лични Данни с цел оценка на личните аспекти на дадена физическо лице, по-специално анализирането или прогнозирането на различни аспекти, имащи отношение към резултатите в работата на субекта на данни, икономическото състояние, здравето, личните предпочитания или интереси, благонадеждността или поведението,_ местоположението или движенията. Профилирането е вид Автоматизирано Обработване.

Администратор: лицето или организацията, която определя кога, защо и как се обработват Лични Данни. Администраторът е отговорен за определяне на практики и политики в съответствие с GDPR. Ние сме Администратор на всички Лични Данни, отнасящи се до нашия Персонал, както и на Лични Данни използвани за нашите собствени търговски цели.

Длъжностно лице по защита на данните (DPO): лицето или организацията, която следва да бъде определена в определени ситуации, регламентирани от GDPR. При липса на задължение за определяне на DPO, този термин означава Мениджър по Защита на Данните или друга длъжност, или екипа по сигурност на данни в организацията, който има отговорност за спазване на законодателството в областта на данните.

ЕИП: 28-те държави-членки на ЕС, както и Исландия, Лихтенщайн и Норвегия

Защита на данните на етапа на проектирането: въвеждане на подходящи технически или организационни мерки по ефективен начин, който да осигури съответствие с GDPR.

Известия по защита на данните: отделни известия, съдържащи информация, предоставяна на Субектите на Данни в момента, в който Организацията събира информация за тях. Тези известия могат да бъдат както общи (напр. адресирани към работници и служители или известия на уебсайта на Организацията), така и отнасящи се до обработване със специфична цел.

Изрично Съгласие: съгласие, което изисква много ясно и определено твърдение (не просто действие)

Име на Организацията: „Съобщително строителство и възстановяване“ ЕАД

Лични Данни: всяка информация, идентифицираща Субект на данни или информация, свързана със Субект на данни, който ние можем да идентифицираме (директно или индиректно) само чрез данните или в комбинация с други идентификатори, които притежаваме или до които имаме достъп. Личните Данни включват Чувствителни Лични Данни и Псевдоминизирани Лични Данни, но изключват Анонимизирани

Лични Данни. Личните Данни могат да се отнасят до факти (например – име, e-mail адрес, местоположение или дата на раждане) или до мнение относно действията или поведението на Субекта на данни.

Нарушение на Защитата на Личните Данни: всяко действие или бездействие, което компрометира сигурността, конфиденциалността или целостта на данните, или на физическите, технически, административни или организационни защити, които ние или нашите подизпълнители използваме, за да ги защитим. Загубата, неоторизираният достъп, предоставяне или получаване на Лични Данни са примери за Нарушение на сигурността.

Обработване на Данни: всяка дейност, която е свързана с използването на Лични Данни. Това включва: получаване, записване, съхранение, извършване на операция или серия от операции с данните като напр. организиране, редактиране, възстановяване, използване, предоставяне, изтриване или унищожаване. Обработването също включва и трансфер на Лични Данни до трети лица.

Общият Регламент за Данните (GDPR): Общият Регламент за Данните ((ЕС) 2016/679). Личните Данни са обект на защитата, определена в GDPR.

Оценка на въздействието: механизми и мерки, използвани за идентифициране на риска, свързан с обработката на данните. Оценката на въздействието следва да бъде извършена за всички ключови системи или програми, свързани с Обработването на Лични Данни.

Персонал: всички работници и служители, и управители, назначени по договор за управление и контрол

Псевдоминизиране: заместването на информация, която директно или индиректно идентифицира физическо лице, с един или повече изкуствени идентификатори ("псевдоними") така че лицето да не може да бъде идентифицирано без достъп до допълнителната информация, която следва да се съхранява отделно и да е поверителна.

Субект на данни: идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано, и чиито Лични Данни ние обработваме.

Съгласие: всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на Субекта на данни, посредством изявление или ясно потвърждаващо действие, което изразява съгласие за обработка на Лични Данни свързани с него.

Чувствителни Лични Данни: информация, разкриваща расовия или етнически произход, политическите мнения, религиозни и други подобни вярвания, членство в синдикални организации, физическото или умствено здравословно състояние, сексуален живот, сексуална ориентация, биометрични или генетични данни, както и Лични Данни отнасящи се до наказателни престъпления и присъди.

2. ВЪВЕДЕНИЕ

Тази политика по защита на данните показва как „Съобщително строителство и възстановяване" ЕАД ("ние", "Организацията") управлява Личните Данни на своите клиенти, доставчици, работници и служители, и други трети лица.

Тези вътрешни правила се прилагат спрямо всички Лични Данни, които Организацията обработва, без значение от това на какъв носител са съхранени или дали са свързани с бивши и настоящи работници и служители, собственици на капитала, или всеки друг Субект на Данни.

Тези вътрешни правила следва да се прилагат спрямо целия Персонал на Организацията. Всички работници и служители следва да прочетат, да се запознаят с и да спазват тази Политика, когато обработват лични данни от името на Организацията и да посетят обучение по нейните изисквания. Тези вътрешни правила показват какви са очакванията към Персонала да осигури спазване на

законодателството от страна на Организацията. Всяко нарушение на тези вътрешни правила може да доведе до дисциплинарни санкции спрямо работника или служителя.

Тези правила са вътрешен документ и не могат да бъдат споделяни с трети лица, клиенти или регулаторни органи без предварително одобрение от Организацията.

3. ОБХВАТ

Правилното и законосъобразно управление на Лични Данни ще осигури доверието в Организацията от страна на клиенти и партньори. Опазването на конфиденциалността и целостта на Личните Данни е ключова отговорност. Организацията може да подлежи на санкция в размер до 20 млн. евро или 4 % процента от световния оборот (което от двете е по-голямо и в зависимост от конкретното нарушение), ако не спази изискванията на GDPR.

Всички съответни структури в Организацията носят отговорност за спазването на тези правила от страна на Персонала и следва да въведат подходящи практики, процеси и обучение.

Ръководството на Организацията е отговорно за контрола по прилагането на тези правила, както и, ако е приложимо, за разработване на свързани политики и други насоки.

Всеки служител на Организацията трябва да се свърже с прекия си ръководител или друг представител на ръководството на Организацията при всякакви въпроси относно приложението на тези правила или, ако имате опасения, че те не се прилагат коректно. Задължително е свързането в следните ситуации:

- Ако не сте сигурни за законовата база, на която може да разчитате при обработка на Лични Данни (*вижте Раздел 5.1 по-долу*)
- Ако трябва да разчитате на Съгласие и/или трябва да осигурите Изрично Съгласие
- Ако трябва да изготвите Известия по Защита на Данните (*вижте Раздел 5.3 по-долу*)
- Ако имате притеснение относно срока на съхранение на Лични Данни, които обработвате
- Ако не сте сигурни какви мерки за сигурност на данните следва да въведете, за да защитите Личните Данни
- Ако установите Нарушение на Защитата на Личните Данни
- Ако не сте сигурни на каква база може да извършите трансфер на Лични Данни извън ЕИП (*вижте Раздел 11 по-долу*)
- Ако имате нужда от съдействие в следствие на постъпила информация, че Субект на данни желае да упражни някое от правата си, съгласно GDPR (*вижте Раздел 12 по-долу*)
- Винаги, когато планирате да стартирате или да промените значително начина, по който извършвате определена операция по Обработване, която може да изисква Оценка на Въздействието (*вижте Раздел 13.5 по-долу*) или възнамерявате да използвате Лични Данни за цели, различни от тези, за които са били събрани
- Ако планирате да извършвате дейности по обработка на Лични Данни, базирани на Автоматизирано Обработване, включително Профилиране и Автоматизирано Вземане на Решения
- Ако имате нужда от съдействие относно спазване на приложимото законодателство спрямо дейности по директен маркетинг (*вижте Раздел 13.6 по-долу*)
- Ако имате нужда от съдействие във връзка с търговски или други договори или в други области във връзка със споделяне на Лични Данни (особено с доставчици и клиенти) (*вижте Раздел 13.7 по-долу*)]

4. ПРИНЦИПИ ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Принципи за защита на Личните Данни в GDPR, които изискват всички Лични Данни:

i. *Да се обработват законосъобразно, добросъвестно и прозрачно*
ii. *Да се събират само за конкретни, изрично оказани и легитимни цели*
iii. *Да бъдат подходящи, свързани с и ограничени до стриктно необходимото за целите, за които се обработват*
iv. *Да бъдат точни и при възможност поддържани в актуален вид*
v. *Да са съхранявани във формат, който да позволява идентифицирането на Субекта на данни за не по-дълъг срок от необходимия за целите на Обработването*
vi. *Да са обработени по начин, който осигурява тяхната сигурност, използвайки технически и организационни мерки, които да ги предпазват от неоторизирано или незаконно Обработване и от случайна загуба, унищожаване или повреждане*
vii. *Да не се трансферират до друга страна извън ЕИП без необходимите предпазни мерки*
viii. *Да се предоставят на Субектите на Данни, на които да се даде възможност да упражнят правата си спрямо техните Лични Данни.*

5. ЗАКОНОСЪОБРАЗНОСТ, ДОБРОСЪВЕСТНОСТ, ПРОЗРАЧНОСТ

5.1.ЗАКОНОСЪОБРАЗНОСТ И ДОБРОСЪВЕСТНОСТ

Личните Данни трябва да се обработват законосъобразно, добросъвестно и по прозрачен начин спрямо Субекта на данни.

GDPR ограничава кръга на нашите действия с Лични Данни до тези, за които е на лице законосъобразна база. Тези ограничения не целят да предотвратят Обработването, а да гарантират, че Личните Данни се обработват добросъвестно и без негативни последствия за Субекта на данни, като регламентира законосъобразните бази за обработка, някои от които са изброени по-долу:

i. *Субектът на данните е дал своето Съгласие*
ii. *Обработването е необходимо във връзка с изпълнението на договор със Субекта на данните*
iii. *Обработването е необходимо, за да изпълним нашите законови задължения*
iv. *Обработването е необходимо, за да се защитят жизненоважните интереси на Субекта на данните*
v. *Обработването е необходимо за целите на легитимните ни интереси, освен когато пред интересите ни преимущество имат интересите или основните права и свободи на Субекта на Данни. Целите, за които обработваме Лични Данни на това основание трябва да са описани в приложимите Известия по Защита на Данните.*

5.2.СЪГЛАСИЕ

Администраторите на данни могат да обработват Лични Данни единствено в случаите, в които поне една от законовите бази в GDPR е налице, което включва и Съгласие.

Субектът на данни е съгласен с Обработването, ако го изрази ясно – чрез изявление или позитивен акт. Съгласието изисква положително действие –предварително отметнати полета за съгласие или бездействие не представляват валидно съгласие. Ако Съгласието за Обработка на Лични Данни се дава чрез документ, който урежда и други въпроси, то следва да бъде изискано отделно от съгласието с другите въпроси.

Субектите на данни трябва да могат лесно да оттеглят Съгласието си за Обработване по всяко време и оттеглянето трябва да бъде уважено своевременно. Съгласието трябва да се изиска отново, ако възнамерявате да обработвате Лични Данни на ново, различно основание, за което Субектът не е дал Съгласие първоначално.

В случаите, когато не може да се разчита на друга законова база за Обработване, Изрично Съгласие е обикновено необходимо при обработка на Чувствителни Лични Данни, при Автоматизирано Вземане на Решения и за трансфер на данни извън ЕИП.

5.3.ПРОЗРАЧНОСТ СПРЯМО СУБЕКТА НА ДАННИ

GDPR изисква от всички Администратори да предоставят детайлна, конкретна информация до Субектите на данни, в зависимост от това дали данните са получени от тях директно или от друг източник. Тази информация трябва да бъде предоставена чрез подходящи Известия по Защита на Данните, които трябва да са лесно достъпни и да използват ясен език, без излишна правна терминология, така че Субектите на данни да могат лесно да ги разберат.

При събиране на Лични Данни директно от Субекта, включително при администриране на трудови правоотношения, на Субекта трябва да се предостави информацията, изисквана от GDPR.

Информацията следва да включва: данни за контакт с Администратора, как и защо ще използваме, обработваме, предоставяме, защитим и съхраним Личните Данни. Организацията предоставя информацията в момента на получаване на Личните Данни от Субекта.

6. ОГРАНИЧЕНИЕ НА ЦЕЛИТЕ

Всички Лични Данни трябва да се съберат само за конкретни и легитимни цели, и не трябва да се обработват по-начин, който не е съвместим с тези цели.

Няма да се използват Лични Данни за нови, различни и несъвместими с първоначалните цели, освен ако Субектът не предостави последващо Съгласие за новите цели.

7. МИНИМИЗИРАНЕ НА ДАННИТЕ

Личните Данни следва да бъдат подходящи, свързани с и ограничени до стриктно необходимото за целите, за които се обработват.

Лични Данни се обработват, само когато това е свързано с изпълнение на служебните задължения на Организацията като се поема ангажимент за осигуряване навременното изтриване/унищожаване или анонимизиране, в съответствие с насоките на Организацията, на всички Лични Данни, които вече не са необходими за конкретните цели.

8. ТОЧНОСТ

Личните Данни, които съхранява Организацията, са точни, пълни, актуализирани и ограничени до целите, за които са събрани. Точността на всички Лични Данни се проверява в момента на тяхното събиране и на регулярни интервали след това. Вземат се всички разумни мерки за унищожаването или корекцията на всички неточни или неактуални Лични Данни.

9. ОГРАНИЧАВАНЕ НА СЪХРАНЕНИЕТО

Личните Данни не бива да се съхраняват във формат, който позволява идентифицирането на Субекта за по-дълго време от необходимото за целите, за които са събрани.

Организацията разработва правила и политики относно съхранението на Лични Данни, които да осигурят изтриване на Данните, за които вече не съществува легитимна цел за Обработване, освен ако друг закон не задължава да се запазят данните за определен минимален срок.

Вземат се всички разумни мерки за унищожаване и изтриване от системите на Организацията на всички Лични Данни, от които вече няма нужда, в съответствие с правилата и политиките по съхранение (вкл. ангажимент за изискване към трети страни да изтрият тези Лични Данни).

10.СИГУРНОСТ, ЦЯЛОСТ И КОНФИДЕНЦИАЛНОСТ

10.1. ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Личните Данни следва да бъдат защитени с необходимите технически и организационни мерки срещу неоторизирано и незаконно Обработване, и срещу случайна загуба, унищожаване или увреждане, за което се разработват, въвеждат и поддържат подходящи мерки за защита, съобразени с дейността на Организацията, нейните ресурси, количеството и вида Лични Данни, които тя обработва.

Всички въведени процедури и технологични мерки се следват, с цел опазване сигурността на Личните Данни от момента на тяхното събиране до момента на тяхното унищожаване. Може да се трансферират лични данни до подизпълнители, само ако те се съгласят да спазват политиките и процедурите на Организацията и да осигурят необходимите мерки за защита, които тя изисква.

Ще се осигури сигурността на данните като се защити тяхната конфиденциалност, цялост и достъпност, дефинирани както следва:

- Конфиденциалност означава, че само хората, които следва да знаят и са оторизирани да използват Личните Данни, имат достъп до тях
- Цялост означава, че Личните Данни са точни и подходящи за употреба за целите, за които се Обработват
- Достъпност означава, че оторизираните потребители имат осигурен достъп до Личните Данни за оторизирани цели.

10.2. ДОКЛАДВАНЕ НА НАРУШЕНИЕ НА ЗАЩИТАТА НА ДАННИТЕ

GDPR изисква от Администраторите да докладват Нарушенията на Защита на Данните пред регулаторния орган и, в някои ситуации, до Субекта на данни.

При спазване на процедурите за идентифициране на подобни нарушения ръководството на Организациията ще уведоми регулатора, и Субекта на данни ако е необходимо, в предвидените от GDPR случаи като съхранява всички доказателства за потенциалното или установено нарушение.

11.ОГРАНИЧАВАНЕ НА ПРЕДАВАНЕТО

GDPR ограничава трансферите на данни до странни извън ЕИП с цел да гарантира пред Субектите, че нивото на защита, гарантирано от GDPR, не е компрометирано като трансфер на Лични Данни извън ЕИП може да се извърши, само ако едно от следните условия е налице:

i. *Европейската Комисия е издала решение, потвърждаващо, че страната, към която се извършва трансфера осигурява адекватно ниво на защита на правата и свободите на Субектите на данни*
ii. *Налице са подходящи мерки за защита – като например Обвързващи Корпоративни Правила (ОКП), стандартни договорни клаузи, одобрени от Европейската Комисия, одобрен кодекс за поведение или сертификационен механизъм*
iii. *Субектът на данни е дал своето Изрично Съгласие за трансфера, след като е информиран за възможните рискове, или*
iv. *Трансферът е необходим за една от целите, изброени в GDPR, включително изпълнението на договор със Субекта, защита на обществения интерес, установяване и защита на правни спорове, защита на жизненоважните интереси на Субекта на данни в случаите, когато той е физически или юридически неспособен да даде съгласие, и в някои ограничени случаи – за защита на легитимните ни интереси.*

12.ПРАВА НА СУБЕКТИТЕ НА ДАННИ И ИСКАНИЯ ЗА ДОСТЪП ДО ДАННИТЕ

Субектите на данни имат права що се отнася до това как се управляват техните Лични Данни, включително право да:

i. *Оттеглят Съгласието си за Обработване по всяко време*
ii. *Получат определена информация за дейностите по Обработване на Администратора*
iii. *Изискат достъп до Личните им Данни, които Обработваме*
iv. *Възразят срещу наша употреба на Личните им Данни за целите на директния маркетинг*
v. *Изискат от нас да изтрием Личните им Данни, ако същите не са вече необходими за целите, за които са събрани или да поправим неточни данни, или да допълним непълни данни*
vi. *Ограничи Обработването в определени ситуации*
vii. *Оспорят Обработване, което е извършено на база защита на нашите легитимни интереси или обществения интерес*
viii. *Изискат копие на договора, въз основа на който Личните им Данни са трансферирани до държава извън ЕИП*
ix. *Възразят срещу решение, взето изцяло на база на Автоматизирано Обработване, включително профилиране*
x. *Бъдат уведомени за Нарушение на Защита на Данните, което е вероятно да доведе до висок риск за техните права и свободи*
xi. *Подадат жалба до регулаторния орган*
xii. *В някои случаи, да получат или да поискат техните Лични Данни да бъдат трансферирани до трета страна в структуриран, общо използван формат, подходящ за машинно четене*

Организацията удостоверява самоличността на лицето, което изисква да упражни някое от правата по-горе.

13.ОТЧЕТНОСТ

13.1. Въвеждане на ефективни технически и организационни мерки, за осигуряване спазването на принципите на защита на данните.

Организацията набавя необходимите ресурси и контролни механизми, за да осигури спазването на изискванията на GDPR, включително:

- Определяне на DPO с подходяща квалификация (когато има такова изискване) и поемане на ръководна отговорност за сигурността на данните
- Въвеждане на защита на данните на етапа на проектиране, когато Обработва Лични Данни и извършва Оценка на Въздействието, когато Обработването представлява висок риск за правата и свободите на Субектите на Данни
- Интегриране на защита на данните във вътрешната си документация
- Осигуряване на регулярно обучение на Персонала по въпросите на защита на данните, като например: права на Субектите на Данни, Съгласие, законова база, Оценка на Въздействието и Нарушение на Защитата на Данни.
- Регулярно тестване на мерките за осигуряване на защита и периодичен одит с цел оценка на ефективността и нивото на спазване

13.2. РЕГИСТРИ

Организацията поддържа актуални регистри, съгласно изискванията на GDPR, отразяващи Обработването, включително регистър на получените Съгласия и процедури по получаване на Съгласията.

Като минимум, тези регистри трябва да включват името и контактната информация на Администратора (и DPO, ако е определен такъв), ясно описание на вида Лични Данни, Субекти на Данни, операции по Обработване, цели на Обработване, трети лица, получатели на Лични Данни (ако има такива), местосъхранение на Лични Данни, трансфери на Лични Данни (ако има такива, срок на съхранение на Лични Данни.

13.3. ОБУЧЕНИЕ И ОДИТ

Организацията осигурява адекватно обучение на Персонала си, което да му помогне да спазва изискванията на GDPR като регулярно тества системите и процесите си.

Организацията участва във всички задължителни обучения по защита на данните и преглежда регулярно контролираните от нея системи и процеси.

13.4. ЗАЩИТА НА ДАННИТЕ НА ЕТАПА НА ПРОЕКТИРАНЕ И ОЦЕНКА НА ВЪЗДЕЙСТВИЕТО

Организацията има задължение да въведе мерки за Защита на Данните на Етапа на Проектиране, когато се Обработват Лични Данни, чрез въвеждане на подходящи технически и организационни мерки.

Организацията преценява какво ниво на Защита на Данните на Етапа на Проектиране е подходящо за всички програми/системи/процеси, които управлява, като има предвид следното:

i. *Използваната технология*
ii. *Разходите по внедряване*
iii. *Вида, обхвата, контекста и целите на Обработването, и*
iv. *Рисковете (от различна степен на вероятност и сериозност) за правата и свободите на Субектите, които произлизат от Обработването*

Администраторите трябва да извършат Оценка на Въздействието за високорискови дейности по Обработване.

Организацията извършва Оценка на Въздействието при всяко въвеждане на ключова система или смяна на бизнес програма, която е свързана с Обработване на Лични Данни, включително:

v. *Първоначалното въвеждане на нови технологии или прехода към нови технологии*
vi. *Автоматизирано Обработване, включително профилиране или Автоматизиране Вземане на Решения*
vii. *Обработване на Чувствителни Лични Данни в голям мащаб*
viii. *Мащабно, систематично наблюдение на публично обществена зона*

Оценката на Въздействието следва да съдържа:

ix. *Описание на Обработването, неговите цели и легитимните цели на Администратора, ако е необходимо;*
x. *Оценка на необходимостта и пропорционалността на Обработването спрямо неговата цел*
xi. *Оценка на риска за лицата и мерките за управление на риска, които са взети*

13.5. АВТОМАТИЗИРАНО ОБРАБОТВАНЕ (ВКЛ. ПРОФИЛИРАНЕ) И АВТОМАТИЗИРАНО ВЗЕМАНЕ НА РЕШЕНИЯ

Автоматизирано Вземане на Решения е забранено, когато решението има правни последици за Субекта на данни, освен ако:

i. *Субектът на данни не е дал Изрично Съгласие*
ii. *Обработването е позволено по закон, или*
iii. *Обработването е необходимо за изпълнение или сключване на договор.*

Ако определени видове Чувствителни Лични Данни се обработват, то тогава основания ii) и iii) не са приложими, но тези Чувствителни Лични Данни могат да бъдат Обработвани, когато това е необходимо (освен, ако могат да бъдат използвани други мерки, които навлизат в по-малка степен в личното пространство на лицето) за целите на съществен обществен интерес – като например превенция на измами.

Ако дадено решение е основано изцяло на база на Автоматизирано Обработване (включително профилиране), тогава Субектите на Данните трябва да бъдат уведомени за правото да възразят срещу това Обработване при първата комуникация с тях. Вниманието на Субектите трябва да бъде изрично насочено към това тяхно право.

Оценка на Въздействието следва да се извърши, винаги когато се предприема Автоматизирано Обработване (включително профилиране) или Автоматизирано Вземане на Решения.

13.6. ДИРЕКТЕН МАРКЕТИНГ

Организацията може да бъде обект на определени правила и закони, когато изпраща маркетингови съобщение до клиенти.

Предварителното съгласие на Субекта на Данни се изисква за електронен директен маркетинг (например, чрез e-mail, sms или автоматизирани обаждания). Налице е ограничено изключение от това правило по отношение на съществуващи клиенти, което позволява на организациите да изпращат маркетингови съобщения, ако:

- са получили контактна информация в течение на продажба
- маркетинговото съобщение се отнася до подобни продукти или услуги, и
  е на лице възможност на лицето да се откаже от бъдещи съобщения, както в момента на предоставяне на Личните Данни, така и във всяко последващо съобщение.

Правото на възражение срещу маркетингови съобщения трябва да бъде изрично представено на Субекта на данни, така че да е лесно отличимо от останалата информация. Възражението срещу маркетингови съобщения трябва да бъде уважено своевременно.

13.7. СПОДЕЛЯНЕ НА ЛИЧНИ ДАННИ

Организацията не споделя Лични Данни с трети лица, освен ако не са налице подходящи защити и договорни взаимоотношения.

Организацията може да споделя Лични Данни, които обработва, с друг служител в Организацията, ако изпълняването на професионалните задължения на получателя изисква достъп до данните.

Организацията може да споделя Лични Данни, които контролира, с трети лица, като например подизпълнители, ако следните условия са изпълнени:

i. Те следва да знаят тази информация с цел да изпълнят услуга по договор
ii. Споделянето на Лични Данни е в съответствие с Изявление по Защита на Данните, което е предоставено на Субекта, и, ако е необходимо, Съгласието на Субекта е предоставено
iii. Третата страна се е съгласила да спази необходимите стандарти за сигурност на данните, политика и процедури
iv. Трансферът е в съответствие с приложимите ограничения за трансфер до страни извън ЕИП, и
v. Е на лице, надлежно сключен, договор за Обработване с подизпълнителя, който отговаря на изискванията на GDPR.

14. ВЛИЗАНЕ В СИЛА И ПРОМЕНИ НА ТЕЗИ ПРАВИЛА

Организацията си запазва правото да променя тези Вътрешни Правила по всяко време и без предупреждение.

Тези Вътрешни Правила влизат в сила от 11.06.2019г.

Утвърдил:

Ивайло Тодоров
Изпълнителен директор на Организацията

ПОЛИТИКА ЗА ВИДЕОНАБЛЮДЕНИЕ

към Вътрешните правила за защина на данните в „Съобщително строителство и възстановяване“ ЕАД

Ние вярваме, че видеонаблюдението е от ключово значение за нашите усилия да осигурим безопасна и сигурна среда за нашите клиенти, служители и партньори. Но също така осъзнаваме, че неговата употреба може да породи известни притеснения относно опазването на личната неприкосновеност на физическите лица, обект на наблюдението.

Изображенията, заснети чрез системите ни за видеонаблюдение, са лични данни и ние ги обработваме съгласно изискванията на българското и европейското законодателството по защита на данните.

„Съобщително строителство и възстановяване" ЕАД (ССВ) е администратор на личните данни, записани чрез системите за видеонаблюдение в Централна управление (ЦУ) и в клоновете на ССВ, и е отговорно за тях. За нас спазването на законовите ни задължения, както и ангажимента ни да уважаваме правата на нашите клиенти, служители и партньори спрямо техните данни, са висок приоритет.

ДЕФИНИЦИИ

Данни: информация, която се съхранява на електронен или хартиен носител. В контекста на видеонаблюдението, данни най-често означава видео записи, но може да включва и снимки.
Лични данни: информация, чрез която дадено живо физическо лице може да бъде идентифицирано. Записите от видео камери също са лични данни.
Системи за видеонаблюдение: всички камери и други технически средства, инсталирани в нашите помещения и използвани с цел да заснемат и запишат изображения на физически лица и нашата собственост.
Субекти на данни: всички живи физически лица, чиито лични данни обработваме в резултат на видеонаблюдение.

ЗА ТАЗИ ПОЛИТИКА

Ние използваме видеонаблюдение, за да наблюдаваме и записваме физическите лица, които се намират на територията на нашите недвижими имоти – по-специално в зоната/зоните около входните пунктове, складовите помещения в предприятието и сградата на ЦУ на ССВ. Целта на тази политика е да разясни как и защо използваме видеонаблюдение, и как обработваме събраните с него личните данни.

Тази политика се прилага както спрямо всички наши служители, така и спрямо всички клиенти, партньори и контрагенти, и всички останали физически лица, които се намират в зоната на наблюдение.

Тази политика ще бъде преглеждана редовно, за да се уверим, че отговоря на законовите изисквания, както и на указанията на Комисията за Защита на Личните Данни.

ПРИЧИНИ ЗА УПОТРЕБАТА НА ВИДЕОНАБЛЮДЕНИЕ

Ние използваме видеонаблюдение по причините описани по-долу. Ние вярваме, че употребата на видеонаблюдение е в нашия легитимен бизнес интерес, по-специално в това да:

- Се опитаме да предотвратим престъпление и да защитим собствеността и активите си;
- Осигурим безопасна и сигурна среда за нашите служители, клиенти, партньори, контрагенти и всички други лица, намиращи се в зоната на видеонаблюдение;
- Подпомогнем органите на реда в предотвратяването, разследването и разкриването на престъпления.

ЗОНА НА НАБЛЮДЕНИЕ

Видеонаблюдението обхваща зоната/зоните около входните пунктове и складовите помещения в ССВ, и сградата на ЦУ на ССВ.

Местоположението на камерите е избрано така, че те да не обхващат зони, които не е необходимо да наблюдаваме, за да осъществим легитимните си цели (описани по-горе).

ОПЕРИРАНЕ НА СИСТЕМИТЕ ЗА ВИДЕОНАБЛЮДЕНИЕ

Ние ще се уверим, че на входа на зоната на наблюдение има поставени знаци, които информират лицата, че техните изображения могат да бъдат записани. Тези знаци дават информация за това, че ние сме отговорни за системата за видеонаблюдение, за целта на наблюдението, както и затова от кого лицата могат да получат повече информация при необходимост.

Ние ще се уверим, че само тези служители или подизпълнители, които са оторизирани от нас, имат достъп до записите от видеонаблюдението.

УПОТРЕБА НА ДАННИТЕ, СЪБРАНИ ЧРЕЗ ВИДЕОНАБЛЮДЕНИЕ

За да се уверим, че законовите права на лицата, заснети от нашите системи за видеонаблюдение, са защитени, ние ще съхраняваме тази информация по начин, който осигурява нейната цялост и сигурност.

Възможно е да предоставим достъп до данните от системите за видеонаблюдение на подизпълнители – обработващи лични данни. В този случай ще се уверим, че имаме разумни договорни гаранции относно запазване на сигурността и целостта на данните от страна на подизпълнителите.

СЪХРАНЕНИЕ НА ДАННИТЕ, СЪБРАНИ ЧРЕЗ ВИДЕОНАБЛЮДЕНИЕ

Данните, събрани чрез нашите системи за видеонаблюдение, се съхраняват на твърди дискове, част от записващите видеосистеми, за срок от около 72 часа след тяхното записване. След изтичане на този срок те ще бъдат перманентно и сигурно заличени.

ПРИКРИТО ВИДЕОНАБЛЮДЕНИЕ

Ние няма да осъществяваме прикрито видеонаблюдение при никакви обстоятелства. Прикрито видеонаблюдение е това наблюдение, при което лицата не са информирани, че са обект на наблюдение.

ПРЕДОСТАВЯНЕ НА ДАННИ

Ние няма да предоставяме данните, събрани чрез системите за видеонаблюдение на трети лица, освен когато това се изисква от нас от органите на реда за целите на разследване или разкриване на престъпление.

Ние ще поддържаме отчетност във всички случаи, в които сме предоставили данни на трети лица.

ИСКАНИЯ ЗА ДОСТЪП

Физическите лица могат да отправят към нас искане за достъп до личната им информация, което може да включва и записи от системите ни за видеонаблюдение. Такова искане следва да бъде отправено писмено.

За да можем да установим кой е записът, който е предмет на постъпилото искане, то искането трябва да включва информация за датата и по възможност часа или часовия диапазон на записване, съответната зона и, ако е необходимо, информация, идентифицираща лицето, което е отправило искането.

В отговора си на такова искане, ние си запазваме правото да замъглим изображенията на трети лица, които присъстват в съответния запис, ако сметнем това за необходимо.

ВЪПРОСИ И ОПЛАКВАНИЯ

Ако имате въпроси относно тази политика или притеснения относно нашата употреба на системите ни за видеонаблюдение, моля обърнете се към дирекция „ФАД“ на ССВ чрез email: office@dpssv.com.

Напомняме Ви, че имате право да подадете оплакване до компетентния регулаторен орган по защита на данните в Република България – Комисията за Защита на Личните Данни.

София, 11.06.2019 г.

Дирекция „ФАД“, ЦУ на ССВ