ПОЛИТИКА ЗА ЗАШИТА НА ЛИЧНИТЕ ДАННИ НА СЛУЖИТЕЛИ

1. Цел, обхват и потребители

Регламент (ЕС) 2016/679 (Общ регламент за защита на данните) замества Директива 95/46/ЕО за защита на данните. Има пряко действие и предполага изменение в законодателството на страните-членки в областта на защитата на личните данни. Неговата цел е да защитава "правата и свободите" на физическите лица и да се гарантира, че личните данни не се обработват без тяхно знание и когато е възможно, че се същите обработва с тяхно съгласие.

Обхват очертан от EU GDPR

Материален обхват (член 2) – настоящият регламент се прилага за обработването на лични данни изцяло или частично с автоматични средства както и за обработването на лични данни с други средства (например ръчно и на хартия), които са част от регистър с лични данни или които са предназначени да съставляват част от регистър с лични данни.

Териториален обхват (член 3) – правилата на Общия Регламент ще важат за всички администратори на лични данни, които са установени в ЕС, които обработват лични данни на физически лица в контекста на своята дейност. Ще се прилагат и за администратори извън ЕС, които обработват лични данни с цел да предлагат стоки и услуги или ако наблюдават поведението на субектите на данни, които пребивават в ЕС.

СОФКОНСУЛТ се стреми да спазва местните закони и регламенти, свързани със защита на личните данни в Р. България и страните, в които организацията може да извършва дейности по партньорски проекти, обмен на кадри и др. Политиката описва основните принципи, съгласно които организацията обработва лични данни за потребители, клиенти, доставчици, търговски партньори, служители и други физически лица и определя отговорностите на своите служители при обработването на личните данни.

Тази политика се прилага за организацията в София, която обработва лични данни на субекти на данни от ЕИО и извън Европейската Икономическа Общност (ЕИО).

Потребители на този документ са всички служители, на постоянна или временна заетост, всички изпълнители, които работят от името на организацията, както и всички клиенти, ползващи услугите на организацията.

2. Референтни документи

- EU GDPR 2016/679 (Регламент (ЕО) 2016/679 на Европейския Парламент и Съвета от 27 април 2016 за защита на физическите лица по отношение на обработката на лични данни и за свободното движение на такива данни, който отменя Директива 95/46/ЕС)
- Закон за местни данъци и такси (ЗМДТ)
- Закон за класифицираната информация
- Данъчно осигурителен и процесуален кодекс
- Политика по информационна сигурност
- Политика за защита на личните данни на служителите
- Политика за запазване на личните данни
- Описание на длъжността Служител по обработка на личните данни
- Указания за дейности по инвентар на данните и обработката им
- Процедура на искане за достъп до данни от субект на данни

- Указания за оценка на въздействието на личните данни
- Процедура за трансгранично прехвърляне на лични данни
- Процедура за уведомяване за нарушение

1. Определения

Долните определения на термините, използвани в този документ, са взети от чл. 4 на Общия регламент за защита на личните данни на ЕС.

Лични данни: Всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („субект на данни"), което може да се идентифицира директно или косвено, в частност посредством препратка към идентификатор като име, идентификационен номер, онлайн идентификатор или до един или повече фактора, специфични за психическото, физическото, генетичното, умственото, икономическото, културното, или социалното състояние на физическото лице.

Чувствителни лични данни: Лични данни, които по характера си са особено чувствителни по отношение на основните права и свободи, трябва да имат специална защита в контекста на обработването им, тъй като обработването може да доведе до значителни рискове за основните права и свободи. Такива лични данни включват лични данни, които разкриват расов или етнически произход, политически пристрастия, религиозни или философски убеждения, членства в профсъюзи, генетични данни, биометрични данни за целите на уникална идентификация на физическо лице, данни за здравословното състояние или данни за сексуалния живот на физическото лице или сексуалната му ориентация.

Администратор на лични данни: Всяко 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 ЕС 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: Физическо или юридическо лице, публичен орган, агенция или друг орган, които обработват лични данни от името на администратор на лични данни.

Обработване: Операция или поредица операции, които се извършват по автоматизиран начин с лични данни или поредица лични данни като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, възпроизвеждане, консултиране, използване, разкриване посредством предаване, разпространяване или предоставяне по друг начин, подреждане или комбиниране, ограничаване, изтриване или унищожаване на данни.

Субект на данните – всяко живо физическо лице, което е предмет на личните данни, съхранявани от Администратора.

Съгласие на субекта на данните - всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени.

Дете: – Общият Регламент определя като дете всеки на възраст под 16 години въпреки, че възрастта може да бъде намалена до 13 г. съгласно правото на страната-членка. Обработката на лични данни на едно дете е законно само, ако родител или попечител е дал съгласие. Администраторът полага разумни усилия, за да провери в такива случаи, че притежателят на родителската отговорност за детето е дал или е упълномощен да даде съгласието си.

Нарушение на сигурността на личните данни - нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин.

Основно място на установяване – седалището на администратора в ЕС ще бъде мястото, в което той взема основните решения за целта и средствата на своите дейности по обработване на данни. По отношение на обработващия лични данни основното му място на установяване в ЕС ще бъде неговият административен център.

Ако администраторът е със седалище извън ЕС, той трябва да назначи свой представител в юрисдикцията, в която администраторът работи, за да действа от името на администратора и да се занимава с надзорните органи. (Член 4 т.16) от EU GDPR.

Анонимизиране: Необратимо деидентифициране на лични данни по начин, по който лицето не може да бъде идентифицирано с използването на време, пари и технологии нито от администратора, нито от друго лице. Принципите за обработване на лични данни не се прилагат за анонимизирани данни, защото те престават да бъдат лични данни.

Псевдоанонимизиране: Обработване на лични данни по начин, по който личните данни вече не могат да бъдат отнесени към конкретен субект на данни без използване на допълнителна информация при условие, че такава допълнителна информация се съхранява отделно и е предмет на технически и организационни мерки, които осигуряват личните данни да не се отнасят до идентифицирано или идентифицируемо физическо лице. Псевдоанонимизирането намалява, но не елиминира напълно възможността личните данни да бъдат свързани със субекта на данни. Тъй като псевдоанонимизираните данни са все още лични данни, обработването на псевдоанонимизирани данни трябва да отговаря на принципите за обработване на личните данни.

Получател - физическо или юридическо лице, публичен орган, агенция или друга структура, пред която се разкриват личните данни, независимо дали е трета страна или не. Същевременно публичните органи, които могат да получават лични данни в рамките на конкретно разследване в съответствие с правото на Съюза или правото на държава членка, не се считат за „получатели"; обработването на тези данни от посочените публични органи отговаря на приложимите правила за защита на данните съобразно целите на обработването;

Трансгранично обработване лични данни: Обработването на лични данни, което става в контекста на дейностите на обект в една или повече страни членки на администратора или обработващия в Европейския Съюз, където са локализирани администраторът или обработващият; или обработване на лични данни, което става в контекста на дейности на отделен обект на администратор или обработващ в ЕС, но значително се отразява на или може да се отрази значително на субекта на данни в една или повече страни членки;

Надзорен орган: Независим публичен орган, който е основан в страна членка съгласно чл. 51 от EU GDPR;

Водещ надзорен орган: Надзорен орган с основна отговорност за за дейностите по обработването на трансгранично обработване на данни, например когато субект на данни подаде оплакване за обработването на негови / нейни лични данни; той е отговорен освен останалото, за получаването на уведомления за нарушаване на данните при дейност по рисково обработване на данни и има всички правомощия по отношение на задълженията си за осигуряване на съответствие с изискванията на EU GDPR;

Всеки "**местен надзорен орган**" ще продължава да поддържа на територията си и да контролира всички обработвани местни данни, които засягат субекти на данни или които се изнасят от администратор или обработващ от ЕС или извън ЕС когато тяхното обработване е свързано със субект на данни, находящ се на територията. Техните права и задачи включват провеждането на проучвания и налагането на административни мерки и глоби, повишават публичното осъзнаване на рисковете, правилата, сигурността и правата за съхранение на обработвани лични данни, както и получаването на достъп до всички помещения на администратора и обработващия, включително всички оборудване и средства за обработване.

"Основен обект на обработващ лични данни" с обекти в повече от една страна членка, мястото на централната му администрация в ЕС, освен ако решенията за целите и средствата за обработване на личните данни не се вземат в друг обект на администратора в ЕС и последният обект има правото да изпълнява такива решения, като в този случай обектът, взел такива решения, се смята за основен обект;

"Основен обект на обработващия лични данни" с обекти в повече от една страна членка, мястото на централната му администрация в ЕС или, ако обработващият няма централна администрация в ЕС, обектът на обработващ в ЕС, където се осъществяват основните дейности по обработването в контекста на дейностите на обекта на обработващия, е предмет на специалните изисквания на регламента;

2. Основни принципи, свързани с обработването на личните данни

Принципите за защита на личните данни очертават основните отговорности за организациите, които обработват лични данни. Чл. 5(2) от GDPR предвижда, че "*администраторът носи отговорност за и може да демонстрира спазване на принципите*."

Личните данни трябва да бъдат обработвани законосъобразно, добросъвестно и прозрачно

Законосъобразно – да идентифицира законна основа, преди да може да обработва лични данни. Те често са посочени като "основания за обработване", например „съгласие".

Добросъвестно - за да може обработването да бъде добросъвестно, администраторът на данни трябва да предостави определена информация на субектите на данни, доколкото това е практически възможно. Това важи независимо дали личните данни са получени директно от субектите на данни или от други източници.

Регламент (ЕС) 2016/679 увеличава изискванията за това каква информация трябва да бъде на разположение на субектите на данни, която е обхваната от изискването за "прозрачност".

Прозрачно – Общият регламент включва правила относно предоставяне на поверителна информация на субектите на данни в членове 12, 13 и 14 от GDPR. Те са подробни и конкретни, поставяйки акцента върху това, че известията за поверителност са разбираеми и достъпни. Информацията трябва да бъде съобщена на субекта на данните в разбираема форма, като се използва ясен и разбираем език.

Специфичната информация, която трябва да бъде предоставена на субекта на данните, трябва да включва като минимум:

- данни, които идентифицират администратора и данните за контакт на администратора и, ако има такъв, на представителя на администратора;
- контактите на ДЛЗД;
- целите на обработването, за което личните данни са предназначени както и правното основание за обработването;

- периода, за който ще се съхраняват личните данни;
- съществуването на следните права - да поиска достъп до данните, коригиране, изтриване (право „да бъдеш забравен“), ограничаване на обработването, както право на възражение срещу условията (или липсата на такива) във връзка с упражняването на тези права;
- категориите лични данни;
- получателите или категориите получатели на лични данни, където това е приложимо;
- където е приложимо, дали администраторът възнамерява да прехвърли личните данни към получател в трета страна и нивото на защита на данните;
- всякаква допълнителна информация, необходима да се гарантира добросъвестно обработване.

1.1. Цялостност и конфиденциалност

Вземайки предвид състоянието на технологиите и останалите мерки за защита, разходите по внедряването, вероятността от настъпване и сериозността на рисковете, свързани с личните данни, дружеството трябва да предприеме необходимите технически и организационни мерки при обработването на личните данни по начин, който гарантира необходимата сигурност на личните данни, включително защита срещу случайно или незаконно унищожаване, загуба, промяна, неупълномощен достъп до или разкриване.

1.2. Отчетност

Администраторът на лични данни носи отговорност за отчетността и трябва да може да демонстрира спазването на гореописаните принципи.

2. Изграждане на защита на данните

С цел доказване на спазването на принципите за защита на личните данни, СОФКОНСУЛТ трябва да изгради защита на данните в своите дейности.

Личните данни трябва да бъдат обработени по начин, който гарантира подходяща сигурност (чл. 24, чл. 32 от ОРЗД).

Отговорникът по защита на данните ще извърши оценка на въздействието (оценка на риска), като вземе предвид всички обстоятелства, свързани с операциите по управление или обработване на данни от организацията. При определянето на това доколко уместно е обработването, Служителят по защита на данните трябва също така да разгледа степента на евентуална вреда или загуба, която може да бъде причинена на физически лица (напр. персонал или клиенти), ако възникне нарушаване на сигурността, както и всяка вероятна вреда за репутацията на администратора, включително евентуална загуба на доверие на клиентите.

При оценяването на подходящи технически мерки, длъжностното лице по защита на данните ще разгледа следното:

- Защита с парола;
- Автоматично заключване на бездействащи работни станции в мрежата;
- Премахване на права на достъп за USB и други преносими носители с памет;
- Антивирусен софтуер и защитни стени;
- Правата за достъп, включително тези на временно назначен персонал
- Защитата на устройства, които напускат помещенията на организацията, като лаптопи или други;
- Сигурност на локални и широкообхватни мрежи;

- Технологии за подобряване на поверителността, като например псевдонимизиране и анонимизиране.
- Идентифициране на подходящи международни стандарти за сигурност подходящи за организацията.

При оценяването на подходящите организационни мерки Служителят по защита на данните ще вземе предвид следното:

- Нивата на подходящо обучение в организацията.
- Мерките, които отчитат надеждността на служителите (например атестационни оценки, препоръки и т.н.).
- Включването на защитата на данните в трудовите договори;
- Идентификация на дисциплинарни мерки за нарушения по отношение на обработването на данни.
- Редовна проверка на персонала за спазване на съответните стандарти за сигурност.
- Контрол на физическия достъп до електронни и хартиено базирани записи.
- Приемането на политика на „чисто работно място“.
- Съхраняване на хартия на базата данни в заключващи се стенни шкафове.
- Ограничаване на използването на портативни електронни устройства извън работното място.
- Ограничаване на използването от служителите на лични устройства на работното място.
- Приемане на ясни правила за създаване и ползване на пароли.
- Редовно създаване на резервни копия на личните данни и физическо съхраняване на носителите с копия извън офиса.
- Налагане на договорни задължения на организации контрагенти да предприемат подходящи мерки за сигурност при прехвърляне на данни извън ЕС.

Тези контроли са избрани въз основа на идентифицираните рискове за лични данни, както и потенциала за нанасяне на вреди, на лицата, чиито данни се обработват.

1.1. Уведомление за субекти на данни

1.2. Личните данни могат да се обработват само след получаване на съгласие от Служителя по защита на данните.

1.3. Дружеството взема решение дали да направи оценка за въздействието на личните данни за всяка дейност по обработване съгласно указанията за оценка на въздействието на личните данни.

1.4. Избор и съгласие на субекта на данни

1.5. Под „съгласие“ организацията ще разбира всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени. Субектът на данните може да оттегли своето съгласие по всяко време.

1.6. Организацията разбира под "съгласие" само случаите, в които субектът на данните е бил напълно информиран за планираното обработване и е изразил своето съгласие и без върху му да бъде упражняван натиск. Съгласието, получено при натиск или въз основа

на подвеждаща информация, няма да бъде валидно основание за обработване на лични данни.

1.7. Съгласието не може да бъде изведено от липсата на отговор на съобщение до субекта на данни. Трябва да има активна комуникация между администратора и субекта, за да е налице съгласие. Администраторът трябва да може да докаже, че е получено съгласие за дейностите по обработване.

1.8. За специални категории данни трябва да се получи изрично писмено съгласие Процедура по получаване на съгласие за обработване на лични данни на субектите на данни, освен ако не съществува алтернативно законно основание за обработване.

1.9. В повечето случаи съгласието за обработка на лични и специални категории данни се получава рутинно от организацията, като се използват стандартни документи за съгласие (посочете) напр. когато нов клиент подписва договор или по време на набиране на нов персонал, справка от ЧР и т.н..

1.10. Ако организацията обработва лични данни на деца, трябва да бъде получено разрешение от упражняващите родителските права (родители, настойници и т. н.). Това изискване се прилага за деца на възраст под 16 години (освен ако държавата-членка не е предвидила по-ниска възрастова граница, която не може да бъде по-ниска от 13 години).

СОФКОНСУЛТ трябва да се стреми да събира минималното необходимо количество лични данни. Ако личните данни се събират от трета страна, Служителят по защита на данните трябва да осигури законното събиране на личните данни.

1.11. Използване, съхранение и разпореждане

Целите, методите, ограниченията за съхраняване и срокът на запазване на личните данни, трябва да отговарят на информацията, съдържаща се в декларацията за поверителност. СОФКОНСУЛТ трябва да осигури точността, целостта, конфиденциалността и съответствието на личните данни за целите на обработването. Трябва да се използват адекватни механизми за сигурност, които имат за цел защита на личните данни с цел предотвратяване на нарушения като кражба, злоупотреба или неправомерна употреба с личните данни. Служителят по защита на данните носи отговорност за спазването на изискванията, изброени в този раздел.

1.12. Разкриване на трети страни

Във всички случаи, в които дружеството използва доставчик трета страна или търговски партньор за обработката на лични данни от негово име, Служителят по защита на данните трябва да осигури обработващият да има въведени мерки за сигурност за защита на личните данни, които съответстват на свързаните с тях рискове Може да включва: злоупотреба с лични данни, упълномощено разкриване на лични данни, нарушаване на лични данни и др. За тази цел трябва да се използват въпросникът за обработващия GDPR и политиката за сигурност на доставчика.

Организацията трябва да изиска по договор доставчикът или търговският партньор да осигурят същото ниво на защита на данните. Доставчикът или търговският партньор трябва да обработват единствено лични данни с цел изпълнение на своите договорни задължения към СОФКОНСУЛТ или съгласно инструкциите на СОФКОНСУЛТ и с никаква друга цел. Когато СОФКОНСУЛТ обработва лични данни заедно с независима трета страна, СОФКОНСУЛТ трябва изрично да посочи своите

съответни задължения и задълженията на третата страна в договор или друг законово обвързващ документ като договор с доставчик на услуги по обработване на данни.

1.13. Прехвърляне на лични данни през граница

Преди да прехвърлите лични данни извън Европейската Икономическа Общност (ЕИО), трябва да въведете адекватни мерки за защита , включително подписване на договор за прехвърляне на данни, както се изисква от Европейския Съюз и, ако се изисква, да получите разрешение от съответния орган по защита на личните данни. Организация, която получава лични данни, трябва да спазва принципите за обработване на личните данни, описани в процедурата за трансграничен трансфер на данни.

1.14. Права на субектите на данни до данни

Когато изпълнява функциите на администратор на лични данни, Служителят по защита на данните е отговорен да осигури субектът на данни да разполага с необходимия механизъм за достъп, за да има достъп до съответните лични данни и да може да ги обновява, коригира, изтрива или прехвърля, ако се налага или се изисква по закон. Механизмът за достъп е описан по-подробно в **процедурата искане за достъп от субект на данни**.

1.15. Преносимост на данни

Субектът на данни има право да получи безплатно копие от данните, които е предоставил, в структуриран формат и да предостави тези данни на друг администратор. Служителят по защита на данните трябва да осигури такива искания да бъдат обработени в срок от един месец, да не бъдат прекалено / Например, субектът на данни изпраща искане до СОФКОНСУЛТ всеки ден/обширни и да не засягат правата на лични данни на други лица. /Искането не трябва да засяга правата на неприкосновеност на други лица./

1.16. Право на забравяне

При поискване, субектът на данни има право да поиска СОФКОНСУЛТ да изтрие личните му данни. Когато СОФКОНСУЛТ изпълнява ролята на администратор, Служителят по защита на данните трябва да предприеме необходимите действия (включително технически мерки) да информира трети страни, които използват или обработват такива данни, да спази такова искане.

2. Указания за справедливо обработване

Личните данни могат да се обработват само след получаване на съгласие от Служителят по защита на данните.

Дружеството взема решение дали да направи оценка за въздействието на личните данни за всяка дейност по обработване съгласно указанията за оценка на въздействието на личните данни.

2.1. Известия до субектите на данни

В момента на събиране или преди събирането на лични данни за някакъв вид дейности по обработване, включително, но не само, справки, такси или други дейности, Служителят по защита на данните носи отговорност да уведоми надлежно субекта на данни за следното: **видовете събирани лични данни, целите на обработване, методите на обработване, правата на субекта на данни по отношение**

на неговите лични данни, срока на съхранение, евентуален международен трансфер на данните, ако данните ще бъдат споделяни с трети страни и мерки за защита на личните данни, взети от организацията. Тази информация се предоставя чрез декларацията за защита на личните данни.

Ако СОФКОНСУЛТ има множество дейности, свързани с обработване на лични данни, трябва да имате отделни декларации, специфични за вида дейност по обработване и категориите събирани лични данни.

Когато лични данни се споделят с трета страна, Служителят по защита на данните трябва да осигури субектът на данни да бъде уведомен за това чрез декларацията за събиране на лични данни.

Когато личните данни се прехвърлят на трета страна съгласно политиката за трансгранично прехвърляне на лични данни, декларацията за защита на личните данни трябва да отразява ясно къде и до кое дружество/публичен орган се прехвърлят личните данни.

Когато се събират чувствителни лични данни, Служителят по обработка на личните данни трябва да осигури Декларацията за защита на личните данни ясно да посочва целите, за които се събират съответните чувствителни лични данни.

2.2. Получаване на съгласия

Когато обработването на личните данни става на основа на съгласието на субекта на данни или на други законови основания, Служителят по защита на данните носи отговорност за съхраняването на записа за съответното съгласие. Служителят по защита на данните носи отговорност да осигури на субекта на данни възможност да даде съгласието си и трябва да информира и осигури такова съгласие (във всички случаи, в които представлява законово основание за обработване) да може да бъде оттеглено по всяко време.

Когато събирането на лични данни се отнася за дете под 16 годишна възраст, Служителят по защита на данните трябва да осигури да има получено съгласие от родителя /Имайте предвид, че чл. 8(2) от GDPR постановява, че "Администраторът трябва да положи усилия да провери дали в тези случаи е дадено съгласие или разрешение от родителя, отговорен за детето с отчитане на необходимата технология"/ преди събирането на данни с формуляра за съгласие от родител.

Когато бъде получено искане за коригиране, промяна или унищожаване на лични данни, Служителят по защита на данните трябва да осигури исканията да се вземат предвид в разумен срок. Служителят по защита на данните трябва да води списък на такива искания

Личните данни могат да се обработват само за целите, за които са събрани. Ако СОФКОНСУЛТ иска да обработва лични данни с друга цел, трябва да поиска съгласието на субекта на данни писмено кратко и ясно. Всяко такова съгласие трябва да включва първо началната цел, за която се събират данните, както и новите или допълнителните цели. Искането трябва да посочва също така и причината, която дава основание за промяна на целите. Служителят по обработка на личните данни носи отговорност за спазване на изискванията на този параграф.

Сега и в бъдеще, Служителят по защита на данните трябва да осигури методите за събиране на данни да отговарят на съответния закон, добри практики и индустриални стандарти.

Служителят по защита на данните носи отговорност за създаването и воденето на регистър с декларацията за защита на личните данни.

3. Организация на отговорностите

Отговорността за осигуряване на правилното обработване на личните данни е на всяко лице, което работи в или с СОФКОНСУЛТ и има достъп до личните данни, обработвани от организацията.

Ключовите отговорности, свързани с обработването на личните данни, е на следните длъжности:

Управител или други лица, които вземат решения за и определят стратегическата линия за защита на личните данни в СОФКОНСУЛТ.

Служителят по обработка на личните данни (DPO) или друг определен служител Напр. правен специалист или лице от ИТ отдела, носи отговорност за управлението на програмата за защита на личните данни и е отговорен за развитието и изпълнението на политиките за защита на личните данни отначало докрай, както са определени в описанието на **длъжността на Служителя по обработка на личните данни**;

Юристът заедно със служителя по обработване на личните данни наблюдава и анализира законите за личните данни и промените в регламентите, разработва изискванията и съдейства за постигане на техните цели, свързани с защита на личните данни.

ИТ мениджърът е отговорен за:

- Осигуряване на това всички системи, услуги и оборудване, използвани за съхранението на данни, да отговарят на приетите стандарти за сигурност.
- Извършване на редовни проверки и сканиране за гарантиране на правилното функциониране на сигурността на хардуера и софтуера.

Отговорник маркетинг е отговорен за:

- Одобряването на всички декларации за защита на личните данни, които придружават електронните и другите писма.
- Отговор на всички запивания, свързани със защита на личните данни от страна на журналисти и медии като вестници.
- Когато е необходимо, работи заедно със Служителя по обработка на личните данни за осигуряване маркетинговите инициативи да са съгласно принципите за защита на личните данни.

Отговорник човешки ресурси е отговорен за:

- Това всички служители да са наясно със зашитата на личните данни на потребителя.
- Организиране на експертизата за защита на личните данни и обучения за разясняване на въпросите за всички служители, които работят с лични данни.
- Цялостна защита на личните данни. Тя трябва да осигури личните данни на служителите да бъдат обработвани съгласно законовите търговски цели на работодателя и нуждите.

Отговорник възлагане е отговорен за прехвърлянето на отговорността за защита на личните данни на доставчиците и подобряване на осведомеността на доставчиците за нивата на защита на личните данни, както и за предаване на изискванията за защита на личните данни на всяка трета страна доставчик, която ги използва. Отдел възлагане трябва да осигури дружеството да си запази правото да одитира доставчиците.

1. Указания за сформиране на водещ надзорен орган

1.1. Необходимост от сформиране на водещ надзорен орган

Идентифицирането на водещ надзорен орган е приложимо само когато СОФКОНСУЛТ извършва трансгранично обработване на лични данни.

Трансгранично прехвърляне на лични данни има в следните случаи:

a) *Обработването на лични данни се прави от СОФКОНСУЛТ в други страни членки на ЕС;*
   или
b) *Обработването на лични данни се прави в отделен обект в ЕС, но принципно засяга или е вероятно в основна степен да засяга субекти на данни в повече от една страна членка.*

Ако СОФКОНСУЛТ има обект само в една страна членка и дейностите по обработване засягат единствено субекти на данни в съответната страна членка, няма необходимост от създаване на водещ надзорен орган. Единственият компетентен орган ще бъде надзорният орган в страната, в която дружеството е законно базирано.

1. Отговор в случай на инциденти на нарушения в личните данни

Когато Служителят по обработка на личните данни разбере за действително или предполагаемо нарушаване на лични данни, Служителят по обработка на личните данни трябва да предприеме вътрешно разследване и съответно, мерки за коригиране навреме съгласно политиката за нарушение на лични данни. В случай, че съществува риск правата и свободите на субект на данни да бъдат нарушени, СОФКОНСУЛТ като администратор на лични данни трябва да уведоми съответните органи по защита на личните данни незабавно и когато е възможно, в срок от 72 часа.

2. Одит и отчетност

Отдел одит или друг приложим отдел носи отговорност за одитиране на степента доколко добре останалите дирекции и отдели прилагат тази политика.

Всеки служител, който нарушава тази политика, подлежи на налагане на дисциплинарни мерки, както и носи гражданска и наказателна отговорност при нарушаване на законите и регламентите.

3. Конфликт на закони

Тази политика е предназначена да осигури спазването на законите и регламентите в обекта и в страните, в които СОФКОНСУЛТ извършва дейност. Ако възникне конфликт между тази политика и приложими закони и регламенти, превес имат последните.

4. Управление на документи, водени на базата на този документ

наименование на записа	място на съхранение	лице, отговорно за съхранението	контролни мерки за защита на записите	срок на съхранение
формуляри за съгласие на субект на данни	интранет	служител по защита на данните	достъп до папката имат само упълномощените лица	10 години
формуляр за оттегляне на	интранет	служител по	достъп до	10

съгласието от субект на данни		защита на данните	папката имат само упълномощените лица	години
формуляр за съгласие на родител	интранет	служител по защита на данните	достъп до папката имат само упълномощените лица	10 години
формуляр за оттегляне на съгласието на родител	интранет	служител по защита на данните	достъп до папката имат само упълномощените лица	10 години
договори с доставчици, които обработват данни	интранет	служител по защита на данните	достъп до папката имат само упълномощените лица	5 години след изтичане на договора
регистър на декларациите за защита на личните данни	интранет	служител по защита на данните	достъп до папката имат само упълномощените лица	постоянно

5. Валидност и управление на документа

Този документ е валиден от 01.06.2018г.

Притежател на този документ е служител по защита на данните, който може да преразглежда и да обновява документа минимум веднъж на година.