КЛУБ МАГЕЛАН ООД

ПОЛИТИКА ЗА СЪХРАНЕНИЕ НА ДАННИ

Версия 02 / 16.05.2019 г.

Утвърдил: ……..

/Иван Василев Иванов/

Съдържание

1. Предназначение, обхват и ползватели

Тази политика определя необходимите периоди на запазване за определени категории лични данни и определя минималните стандарти, които да се прилагат при унищожаване на определена информация в Клуб Магелан ООД (наричано по-нататък: "Дружеството").

Тази политика важи за всички бизнес единици, процеси и системи във всички държави, в които Дружеството осъществява дейност и има взаимоотношения, или други бизнес отношения с трети страни.

Тази политика важи за всички директори, служители, агенти, филиали, контрагенти, консултанти, консултанти или доставчици на услуги, които могат да събират, обработват или имат достъп до данни (включително лични данни и/или чувствителни лични данни). Отговорност на всички гореизброени е да се запознаят с тази политика и да гарантира адекватното й спазване.

Тези правила се отнасят за цялата информация, използвана в дружеството. Примери за използвани документи:

- Имейли
- Хартиени документи
- Електронни документи
- Видео или Аудио
- Данни, генерирани от системи за физически контрол на достъпа

2. Референтни Документи

- EU GDPR 2016/679 (Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. за защита на физическите лица при обработването на лични данни и за свободното движение на такива данни и за отмяна на Директива 95/46 / ЕО)
- Съответното национално законодателство или правило за прилагане на GDPR
- Други местни закони и разпоредби
- Политика за Защита на Личните Данни

3. Правила за Съхранение

3.1. Основни Принципи на Съхранението

В случай, че някоя от категориите документи, които не са конкретно определени другаде в настоящата Политика (и по-специално в Графика за съхранение на данни) и освен ако не е уредена по различен начин от приложимото законодателство, изискваният период на съхранение за такъв документ ще се счита за 5 години от датата на създаване на документа. Помещенията, определени за архивохранилища, трябва да отговарят на следните оптимални изисквания:

1. Да са пожарообезопасени, да бъдат сухи, леснопроветриви и изолирани

2. Пространствената подредба да осигурява лесен и удобен достъп до съхраняваните документи;

3. Да са с осигурени със средства за ограничаване на физическия достъп чрез надеждни заключващи системи и със средства за авариен достъп.

Помещенията определени за съхраняване на данни следва да отговарят на изискванията за Data center, като:

1. Напълно подсигурено AC/DC захранване – 2 независими източника, подсигурени с дизелови генератори
2. Професионална система за управление и мониторинг
3. Система за околна среда close control, гарантираща постоянни параметри на въздуха – температура 22˚C, влажност 50%
4. Противопожарна система
5. СОТ видеонаблюдение и гарантирана сигурност на достъпа с картова система
6. Комуникационна свързаност – 2 независими трасета минаващи през независими шахти и терминиращи в отделени Meet-me (MMR) стаи

Общ График за Съхранение

Управителя определя периода на съхранение на документи и електронни записи чрез Общия График за Съхранение.

Като изключение, периодите на съхранение в Графика за съхранение на данни могат да бъдат удължени в случаи като:

- Текущи разследвания от страна на органите на държавите-членки, ако има възможност регистрирани лични данни, необходими на Дружеството, да докажат спазването на законови изисквания;
  или
- При упражняване на законни права, в случаи на съдебни дела или подобни съдебни производства, признати от местното законодателство.

a. Защита на данните през периода на съхранение

Трябва да се обмисли възможността за износване на носителите за данни, използвани за архивиране. Ако се избират електронни носители за съхранение, се съхраняват и всички процедури и системи, гарантиращи достъп до информацията през периода на съхранение (както по отношение на информационния носител, така и по отношение на четивността на форматите), за да се запази информацията срещу загубата в резултат на бъдещи технологични промени. Отговорността за съхранението се пада на ИТ отговорника.

b. Унищожаване на данни

Компанията и нейните служители трябва редовно да преглеждат всички данни, съхранявани електронно на свои устройства или на хартия, за да решат дали да унищожат или да изтрият всички данни, след като целта, за която са създадени тези документи, вече не е от значение. Вижте Приложение за графика за запазване. Цялостната отговорност за унищожаването на данни се пада ИТ отговорника под контрола на Управителя.

След като бъде взето решение за разпореждане съгласно Графика за Съхранение, данните трябва да бъдат заличени, нарязани или по друг начин унищожени до степен, равна на тяхната стойност за другите и степента им на поверителност. Методът на унищожаване варира и зависи от естеството на документа. Например, всички документи, които съдържат чувствителна или поверителна информация (и особено чувствителни лични данни), трябва да бъдат унищожени като поверителни отпадъци и да бъдат предмет на сигурно изтриване по електронен път; някои изтекли или заменени договори могат да бъдат раздробени (шредер) вътрешно. В раздела "График за изхвърляне на документи" по-долу е посочен начина на унищожаване.

В този контекст, служителят който изпълнява задачите, трябва да поема подходящите отговорности, свързани с унищожаването на информацията. Специфичният процес на заличаване или унищожаване може да се извърши или от служител, или от вътрешен или външен доставчик на услуги, на който ИТ отговорника възлага изпълнението. Прилагат се всички приложими общи разпоредби, съгласно съответните закони за защита на данните и Политиката за защита на личните данни на компанията.

Трябва да е наличен подходящ и адекватен контрол, който да предотвратява трайната загуба на съществена информация на компанията, в резултат на злонамерено или неволно унищожаване на информацията - тези контроли са описани в Политиките за Сигурност на Информацията.

ИТ отговорника е отговорен за документирането и одобряването на процеса на унищожаване. Приложимите законови изисквания за унищожаване на информацията, се спазват изцяло, като Управителя изцяло съблюдава процеса.

c. Нарушения, Изпълнение и Съответствие

Управителя носи отговорността да гарантира, че всеки от офисите на компанията спазва тази политика. Отговорност на ДЗЛД да подпомага всяка местна или национална служба относно запитвания, касаещи защита на данните на местно или национално ниво.

Всяко подозрение за нарушение на тази Политика трябва да бъде незабавно докладвано на ДЗЛД. Всички случаи на предполагаеми нарушения на Политиката се разследват и се предприемат съответните действия.

Неспазването на тази Политика може да доведе до неблагоприятни последици, включително, но не само: загуба на доверие на клиентите, съдебни спорове и загуба на конкурентно предимство, финансови загуби и щети за репутацията на Дружеството, лични вреди или загуби. Неспазването на тази Политика от постоянни, временни или договорно наети служители или

трети лица, на които е предоставен достъп до помещенията или информацията на Дружеството, може да доведе до дисциплинарно наказание или прекратяване на трудовото им правоотношение или договора. Това несъответствие може също да доведе до съдебни действия срещу страните, участващи в такива дейности.

7. Унищожаване на Документи

a. Рутинен График за Унищожение

Документите съдържащи лични данни, които могат рутинно да бъдат унищожени, освен ако не са предмет на текущо правно или регулаторно разследване, са както следва:

- Обявления и съобщения за ежедневни срещи и други събития;
- Искания за обикновена информация, например указания за пътуване;
- Резервации за вътрешни срещи/външни разходи;
- Документи за предаване като писма, листовки за факсове, имейл съобщения, листове за маршрутизиране, комплименти и други подобни, които придружават документите, но не добавят стойност;
- Съобщения;
- Остарели списъци с адреси, листове за дистрибуция и др.;
- Дублирани документи като CC и копия FYI, непроменени чертежи, разпечатки на снимки или извлечения от бази данни и файлове;
- Стандартни публикации, които са остарели или заменени; и
- Търговски списания, каталози на продавачи, листовки и бюлетини от търговци или други външни организации.
- Досиета на кандидати за работа, които не са били одобрени при направения подбор.

Във всички случаи, унищожението е предмет на изисквания за оповестяване, които могат да съществуват в контекста на съдебни спорове.

b. Методи за унищожение

Документите от Ниво I са тези, които съдържат информация, която е с най-висока степен на сигурност и поверителност, и тези, които включват лични данни. Тези документи се унищожават като поверителни отпадъци (нарязани и изгаряни) и подлежат на защитено електронно изтриване. Изхвърлянето на документите трябва да включва доказателство за унищожаване.

Документите от Ниво II са патентовани документи, съдържащи поверителна информация, като имена, подписи и адреси на страните или които могат да бъдат използвани от трети страни за извършване на измами, но които не съдържат никакви лични данни. Документите трябва да бъдат нарязани и след това да бъдат поставени в заключени контейнери за боклук за събиране

от одобрена фирма. Електронните документи ще бъдат предмет на сигурно електронно изтриване.

Документите от Ниво III са тези, които не съдържат поверителна информация или лични данни и се публикуват във фирмени документи. Те трябва да бъдат раздробени или изхвърлени, чрез компания за рециклиране и да включват, наред с други неща, реклами, каталози, листовки и бюлетини. Те могат да бъдат изхвърляни без запис за това.

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

Име на записа	Място на съхранение	Отговорник за съхранението	Контроли за защита на записите	Време за съхранение
График за Съхранение на данни	Защитен файлов сървър	Управител	Само упълномощени служители имат достъп по формулярите]	Постоянен

9. Валидност и управление на документи

Този документ е валиден от 16.05.2019.

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

10.Приложения

- Приложение – График за Съхранение на Данни

Управител
Иван Василев Иванов

_____

[Подпис]