GG LAW
WE CARE FOR YOUR SUCCESS

02-992 40 58

office@gglaw.bg
www.gglaw.bg

гр. София 1000,
ул. Цар Шишман №3, ет.1
„Господинов и Генчев“

ДОКУМЕНТАЦИЯ ЗА ЗАЩИТА НА ДАННИТЕ ОТ „ОДО ПРО“ ООД

I. ПРЕДМЕТ

Чл. 1. Настоящата документация за защита на Данните, наричана по-долу за краткост “Документация”, представлява споразумение за обработка на лични данни на всички Клиенти на „ОДО ПРО“ ООД, които използват Услугите в съответствие с ИНДИВИДУАЛЕН ДОГОВОР ЗА ВНЕДРЯВАНЕ И ПОЛЗВАНЕ НА СИСТЕМАТА ODOO ERP („Договора“) и приложенията към него.

II. ДЕФИНИЦИИ

Чл. 2. За целите на настоящата Документация страните определиха следните дефиниции:

(1) Администратор на лични данни (Администратор) - е 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. Клиентите на Администратора, предоставящи Лични данни за целите на Договора, ще бъдат считани за Администратори на лични данни, изпълняващи, в това им качество, съответните им законови задължения.

(2) Цели на обработката (Целите) – осигуряване на Клиентите на „ОДО ПРО“ ООД на Услугите, както и обработка с цел бизнес кореспонденция.

(3) „Лични данни (Данни)“ – всяка информация, свързана с идентифицирано физическо лице или физическо лице, което може да бъде идентифицирано („Субект на данни“), 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. Доколкото друго не е уговорено писмено, Данните, предмет на тази Документация, са бази данни или отделни записи информация с Лични данни, генерирани в рамките на осигурените от Услугите стандартни функционалности. Извън данните от предходното изречение, в Обработващият обработва данни на служители на Администратора за цели, посочени в тази Документация.

(4) „Обработващ лични данни (Обработващ)“ - означава физическо или юридическо лице, публичен орган, агенция или друга структура, която обработва лични данни от името на Администратора.

(5) „Обработване на лични данни (Обработването)“ – 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,

02-992 40 58

office@gglaw.bg
www.gglaw.bg

гр. София 1000,
ул. Цар Шишман №3, ет.1
„Господинов и Генчев“

извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване.

III. ЦЕЛИ И ПРЕДМЕТ НА ОБРАБОТВАНЕТО

Чл. 3. Договорът представлява основният правен акт, на чиято база се извършва Обработването.

Чл. 4. За целите на изпълнението на задълженията по Договора Администраторът може да възложи на „ОДО ПРО“ ООД Обработване на лични данни, при което „ОДО ПРО“ ООД ще придобие качеството на Обработващ лични данни от името на Администратора.

Чл. 5. Обработващият ще Обработва лични данни на определени служители, партньори, доставчици, сътрудници и други свързани лица на Администратора на основание законен интерес и с цел осъществяване на бизнес кореспонденция във връзка с:

(1) сключване на договори и извършване на всякакви други правно валидни актове;
(2) предоставяне на Услугите;
(3) проверка на клиентско удовлетворение във връзка с осигурените Услуги;
(4) информация по отношение на Услугите;
(5) новости във връзка с Услугите;
(6) друга полезна информация, отнасяща се до Услугите.

IV. ПРАВА И ЗАДЪЛЖЕНИЯ НА АДМИНИСТРАТОРА

Чл. 6. Администраторът определя целите, предмета и средствата за обработката на Данните, които Обработващият обработва от негово име и във връзка с отношенията между Администратора и Субектите на данни.

Чл. 7. Администраторът се задължава да информира Обработващия преди всяко обработване за цели, които не са предвидени в настоящата Документация.

Чл. 8. Администраторът се задължава да:

(1) предоставя единствено такива Данни, които сам събира и обработва законосъобразно, в качеството си на Администратор или Обработващ, като гарантира, че има валидно правно основание за съответното обработване, съдържанието на Данните не е незаконно и обработването, което извършва, не нарушава права на трети страни;
(2) осигурява писмени указания относно обработването на предоставяните на Обработващия Лични данни, а също така и относно разпорежданията след приключване на услугите по обработване, относими към преследваните цели;

02-992 40 58

office@gglaw.bg
www.gglaw.bg

гр. София 1000,
ул. Цар Шишман №3, ет.1
„Господинов и Генчев“

(3) съдейства на Обработващият, доколкото е възможно и необходимо, при осигуряване спазването на правилата, законите за защита на личните данни и настоящата Документация.

V. ПРАВА И ЗАДЪЛЖЕНИЯ НА ОБРАБОТВАЩИЯ

Чл. 9. Обработващият се задължава да обработва Лични данни от името на Администратора в съответствие с целта и условията, определени в настоящата Документация и при спазване на задълженията за сигурност и защита на Личните данни, съгласно Регламента и законите за защита на личните данни.

Чл. 10. Обработващият се съгласява да се въздържа от използването на Данните за каквато и да е друга цел, различна от посочената от Администратора.

Чл. 11. Обработващият може в рамките на настоящата Документация да ангажира друг Обработващ, като гарантира, че избраният от него Обработващ лични данни се е съгласил писмено със същите задължения.

Чл. 12. Служителите на Обработващият, които извършват операциите по обработка са:

(1) оправомощени да обработват личните данни;
(2) обвързани със съответните споразумения за поверителност;
(3) спазват съответните законови задължения за поверителност, където такива са приложими.
(4) преминали първоначално и периодично обучение и/или инструктаж във връзка с практическото приложение на нормативната уредба относно защита на личните данни;

Чл. 13. Обработващият гарантира, че поддържа и ще продължи да поддържа подходящи и достатъчни Технически и организационни мерки за сигурност, както са описани в Приложение II към настоящата Документация, за да предпази Данните от случайно или незаконосъобразно унищожаване или случайна загуба, или достъп до тях.

Чл. 14. След предоставяне на Услугите, Обработващият, по избор на Администратора или Субекта на данни:

(1) Заличава всички Лични данни, както и техните копия, освен ако друго не се налага за изпълнение на негови законови задължения;
(2) Връща на Администратора/Субекта на данни всички Лични данни, които той е посочил и заличава съществуващите им копия, освен ако друго не се налага за изпълнение на негови законови задължения.

Чл. 15. В случай, че Администраторът или Субектът на данни не посочи връщане или заличаване на данните, Обработващият може да съхрани част или всички от Данните за срок не по-дълъг от 5 години, следващи годината на фактуриране на

02-992 40 58

office@gglaw.bg
www.gglaw.bg

гр. София 1000,
ул. Цар Шишман №3, ет.1
„Господинов и Генчев“

Услуги, с цел отчетност, контрол по изпълнение на услугите и защита на собствените си законни интереси.

Чл. 16. Обработващият няма право да изтрива и/или запазва Лични данни без изричното документирано указание на Администратора за това.

Чл. 17. Обработващият няма право да предава Лични данни, предоставени от Администраторът или Субекта на данни, на трета държава или международна организация, освен когато това представлява задължение по силата на закон, който се прилага спрямо Обработващия, като в този случай Обработващият ще информира Администратора или Субекта на данни за това правно изискване преди обработването, освен ако това право забранява такова информиране на важни основания от публичен интерес.

VI. СРОК

Чл. 18. Срокът на Обработването по настоящата Документация, съвпада със срока на действие на Договора, освен ако целите на обработването не се изпълнят по някаква причина и по-рано.

Чл. 19. След този срок могат да се обработват единствено Данните, които следва да се съхраняват и след този срок на законово основание и/или по изрично указание на Администратора, при спазване на действащото законодателство в областта на личните данни.

Чл. 20.

VII. ОТГОВОРНОСТ

Чл. 21. Обработващият и Администраторът спазват действащото законодателство в областта на личните данни и изпълняват задълженията си по настоящата Документация по начин, че да не нарушават което и да е от законовите си задължения.

Чл. 22. Администраторът носи отговорност за всички свои указания към Обработващия и спазването на определените от него цели и предмет на обработването, както и за осигуряване правата на Субектите на лични данни.

Чл. 23. Преди започване на обработването и по всяко време след това Обработващият незабавно уведомява Администратора, ако, до колкото му е известно, което и да е документирано указание на Администратора нарушава действащото законодателство в областта на личните данни.

02-992 40 58

office@gglaw.bg
www.gglaw.bg

гр. София 1000,
ул. Цар Шишман №3, ет.1
„Господинов и Генчев“

VIII. ЗАДЪЛЖЕНИЕ ЗА ДОКЛАД

Чл. 24. В допълнение към другите задължения, предвидени в настоящата Документация, Обработващият се задължава незабавно да уведоми Администратора за:

(1) всяко правно обвързващо искане за разкриване на лични данни от правоприлагащ орган, съдилища и компетентни регулаторни органи и други власти, освен ако не е забранено по друг начин.
(2) оплаквания или искания, получени директно от Субекта на данните, без да отговаря на това искане, освен ако Обработващият не е бил по друг начин упълномощен за това, или ако това не се изисква по друг начин от приложимото законодателство.
(3) всяко нарушение на сигурността, касаещо Данните.

Чл. 25. Уведомлението по предходния член включва всички елементи определени в член 33, ал. 3 от GDPR и в допълнение каквато и да е друга информация, която Обработващия прецени, че е необходима, веднага след като такава информация може да бъде събрана или стане достъпна за Обработващия.

Чл. 26. Във всеки случай, Обработващият трябва да съобщи на Администратора в рамките на максимум ... часа, че е настъпило нарушение на сигурността. В следващите максимум ... часа Обработващият трябва да събере и предостави на Администратора следната подробна информация:

(1) вид на нарушението,
(2) естеството, чувствителността и обема на въздействието върху Данните,
(3) улесняване на идентифицирането на лицата,
(4) сериозността на евентуалните или настъпили последици за Субектите на данни,
(5) списък на Субектите на данни, засегнати от нарушението на сигурността, включително информация за контакт,
(6) категориите и приблизителният брой на засегнатите субекти на данни, както и категориите и приблизителният брой на засегнатите записи на лични данни;
(7) вероятните последствия за Администратора от нарушението на сигурността при Обработващия и/или при неговите Подизпълнители;
(8) мерките, които са предприети или трябва да бъдат предприети за справяне с нарушението на сигурността, за смекчаване на последиците и за свеждане до минимум на щетите, произтичащи от нарушението на сигурността.

Чл. 27. След консултация с Администратора, Обработващият предприема незабавни действия за разследване и отстраняване на нарушението на сигурността с цел да установи, предотврати и положи всички усилия за да намали ефекта от такова нарушение.

02-992 40 58

office@gglaw.bg
www.gglaw.bg

гр. София 1000,
ул. Цар Шишман №3, ет.1
„Господинов и Генчев“

(1) Обработващият няма да дава информация на трети лица за нарушението, освен ако съществува вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица.
(2) При необходимост от такова уведомяване Обработващият ще съдейства на Администратора за изпълнението му.

IX. СЪДЕЙСТВИЕ И ПРАВО НА ОДИТ

Чл. 28. Обработващият се задължава да осигури достъп на Администратора до цялата информация, необходима за доказване на изпълнението на задълженията, и да позволява и допринася за извършването на одити, включително проверки, от страна на Администратора или друг одитор, оправомощен от Администратора, след отправяне на изрично писмено искане за това от страна на Администратора до Обработващия.

Чл. 29. Обработващият предоставя писмени отговори на всички разумни искания на Администратора и може да начисли такса за всеки преглед или одит. Обработващият ще предостави подробна информация за всяка приложима такса преди всеки такъв одит и Администраторът ще носи отговорност за всички такси, начислени от всеки одитор, и за всички такси, свързани с извършването на одит. Докладите от всеки такъв одит ще бъдат предоставени на Обработващия без ограничения на целите за по-нататъшното им използване.

Чл. 30. Обработващият може да възрази и да откаже в писмен вид на Администратора или на одитор, назначен от Администратора, да извърши какъвто и да е одит, ако Администраторът или одиторът, по разумно мнение на Обработващия, не е подходящо квалифициран или независим, или е конкурент на Обработващия, или по друг начин е явно неподходящ.

Чл. 31. Обработващият незабавно уведомява Администратора, ако според него дадено указание нарушава Регламента или други разпоредби на ЕС или на държавите членки относно защитата на данни.

Чл. 32. В съответствие с изискванията за сигурност, Обработващият ще допуска, след предварителна писмена уговорка и доколкото това няма да нарушава работния му процес, одит по спазване на гаранциите за сигурност, извършвани от страна на Администратора или от страна на независими трети страни, упълномощени за тези одити от Администратора.

(1) Извършването на одитите и други свързани проверки по тази точка се осъществяват за сметка на лицата, изискващи тези действия.

Чл. 33. Доказателство за спазването на задълженията на Обработващия може да бъде предоставено чрез:

(1) Спазване на одобрени Кодекси за поведение, съгласно член 40 от ОРЗД (ако такива са налични);

02-992 40 58

office@gglaw.bg
www.gglaw.bg

гр. София 1000,
ул. Цар Шишман №3, ет.1
„Господинов и Генчев“

(2) Сертифициране, съгласно одобрена процедура за сертифициране, в съответствие с член 42 от ОРЗД;
(3) Съобразяването със Стандартни договорни клаузи, съгласно член 28 (6) от ОРЗД;
(4) Удостоверяване от одитор; доклади или извадки от доклади, предоставени от независими органи (напр. одитор, Длъжностно лице по защита на данните, отдел за информационна сигурност, одитор за поверителност на данни, одитор за качество и др.)
(5) Подходящо удостоверяване от информационна сигурност или одит за защита на данни (напр. ISO/IEC 27001).

Чл. 34. За целите на настоящата Документация, Обработващият редовно изпитва, преценява и оценява ефективността на техническите и организационните мерки, гарантиращи сигурността на обработката.

Чл. 35. Констатациите по отношение на извършения одит ще бъдат обсъдени и оценени от страните.

X. ПОДИЗПЪЛНИТЕЛИ

Чл. 36. Страните се съгласяват, че в случай на използване на Подизпълнители, ще се прилагат правилата, определени в Приложение III.

XI. ИЗМЕНЕНИЕ И ПРЕКРАТЯВАНЕ

Чл. 37. Обработването на Лични данни може да бъде прекратено:

(1) с изтичането на срока, предвиден в настоящата Документация;
(2) по взаимно съгласие, изразено писмено;
(3) при неизпълнение на задълженията на всяка от страните, както и при нарушения на Общия регламент, като в този случай всяка от страните има право да уведоми надзорния орган за извършеното нарушение.

Чл. 38. Клаузите на настоящата Документация могат да бъдат изменени по взаимно съгласие на страните.

XII. ПРАВА НА СУБЕКТИТЕ НА ДАННИ

Чл. 39. Субектите на лични данни имат правото:

(1) да получат информация относно Обработването на личните им данни.
(2) да поискат коригиране, изтриване, ограничаване използването или блокиране на личните им данни.
(3) на пренос на данни.
(4) на възражение.

Чл. 40. Субектите на лични данни имат правата, свързани с автоматизираното вземане на решения, включително профилиране, съгласно ОРЗД.

02-992 40 58

office@gglaw.bg
www.gglaw.bg

гр. София 1000,
ул. Цар Шишман №3, ет.1
„Господинов и Генчев“

Чл. 41. Страните се съгласяват при получаване на искане за упражняване на права, Обработващият да съдейства и да осигури разумна и бърза помощ (в рамките на 7 дни), за да могат да се уважат исканията за упражняване правата на Субектите на данни и да отговорят на всякакви други запитвания или жалби от Субектите на лични данни.

XIII. ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

Чл. 42. Обработващият и Администраторът спазват правните изисквания за назначаване на длъжностно лице по защита на данни, съгласно член 37 ОРЗД, ако се окаже, че такова е задължително необходимо.

Чл. 43. Настоящата Документация, заедно с приложенията към нея, представлява неразделна част от Договора. За всички неуредени в настоящата Документация правила се прилагат ОУ.

02-992 40 58

office@gglaw.bg
www.gglaw.bg

гр. София 1000,
ул. Цар Шишман №3, ет.1
„Господинов и Генчев“

ПРИЛОЖЕНИЕ I КЪМ ДОКУМЕНТАЦИЯ ЗА ЗАЩИТА НА ДАННИТЕ ОТ „ОДО ПРО“ ООД

Чл. 1. Страните се съгласяват, че Администраторът на лични данни може да поръча обработването на голямо разнообразие от лични данни, свързани с изпълнението на Договора, поради което не би било възможно да се очертаят предварително всички Субекти на данни и категории лични данни на посочените Субекти на данни, които ще бъдат обработвани. По-долу са изброени повечето видове лични данни, които ще бъдат обработвани от Обработващия, както и съответните Субекти на данни.

Чл. 2. Видове лични данни, които ще бъдат обработвани в обхвата на Документацията:

(1) Лична информация за контакт, включително имена, наименование на компанията, имейл адреси, физически адреси и телефонни номера;
(2) Данни за човешките ресурси, като име на работодателя, длъжност, заплата, трудови задължения и допълнителни социални придобивки, когато е приложимо;
(3) Лични данни, необходими за изпълнение на законови задължения към системата за социална сигурност, и други данни за заетостта;
(4) Лични данни, свързани с образование и професионална квалификация.
(5) Администраторът на данни и Обработващият данни потвърждават, че специалните категории Лични данни ще бъдат обработвани само ако и доколкото са посочени в Споразумението.

Чл. 3. Категории Субекти на данни, чиито лични данни ще бъдат обработвани:

(1) Физически лица, които имат достъп до и/или използват Услугите, въз основа на сключения Договор.
(2) Физически лица, чиито данни се предоставят на Обработващия чрез Услугите от или по указание на Администратора или негови Клиенти.
(3) Служители, агенти, лица на свободна практика, Клиенти и други изпълнители на Администратора, както и всички други лица, чиито Лични данни се обработват във връзка с предоставянето на Услугите;
(4) Лица, които предават данни чрез Услугите, включително лица, които си сътрудничат и комуникират с Администратора.

ПРИЛОЖЕНИЕ II КЪМ

02-992 40 58

office@gglaw.bg
www.gglaw.bg

гр. София 1000,
ул. Цар Шишман №3, ет.1
„Господинов и Генчев“

ДОКУМЕНТАЦИЯ ЗА ЗАЩИТА НА ДАННИТЕ ОТ „ОДО ПРО“ ООД

I. СИГУРНОСТ

Чл. 1. Обработващият е отговорен за сигурността на Личните данни, като е задължен да прилага подходящи технически и организационни мерки за защита.

Чл. 2. Обработващият гарантира за постоянно приложение на системи за управление на качеството чрез:

(1) регулярни одити от страна на външни организации, работещи при условията на спазвани споразумения за конфиденциалност;
(2) редовни, както и внезапни вътрешни проверки по спазване на техническите и организационни мерки, установени за роли на всяко ниво в организацията;
(3) предварителен, текущ и последващ контрол по прилагане на изградените политики за сигурност, както и съответните за всяка дейност инструкции за извършване на дейностите по обработка;
(4) предварително извършена оценка на риска по отношение на всяка дейност и съобразяване на резултатите с организацията на дейността.

II. ТЕХНИЧЕСКИ И ОРГАНИЗАЦИОННИ МЕРКИ ЗА СИГУРНОСТ НА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Чл. 3. За целите на настоящата Документация Обработващият предприема технически и организационни мерки за сигурност и защита на Личните данни, съгласно описаното в настоящото Приложение II.

Чл. 4. Обработващият се задължава:

(1) да предотвратява неоторизиран достъп на лица без разрешение до Личните данни и до начините на тяхното обработване;
(2) да предотвратява всяко неразрешено гледане, създаване, копиране, прехвърляне, промяна или изтриване на записи/файлове, съдържащи Лични данни;
(3) да приема мерки, които му позволяват да идентифицира и проверява на кого са прехвърлени Лични данни;
(4) да приема политики, уреждащи правилата за достъп и по-нататъшна обработка на Личните данни.
(5) да изгражда системни и одитни пътеки;
(6) да използва сигурни пароли, двуфакторно удостоверяване, SSH ключове, процеси на оторизация, процеси на управление на промените, технологии за откриване на проникване в мрежата, технологии за криптиране и удостоверяване, процедури за сигурно влизане в системата и защита от вируси;

02-992 40 58

office@gglaw.bg
www.gglaw.bg

гр. София 1000,
ул. Цар Шишман №3, ет.1
„Господинов и Генчев“

(7) да отчита всички рискове, свързани с обработката, например от случайно или незаконно унищожаване, загуба или промяна, неразрешено или незаконно съхранение, обработка, достъп или разкриване на Лични данни;
(8) да осигури псевдонимизация и/или криптиране на Личните данни, когато е уместно;
(9) да поддържа способността за осигуряване на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработка;
(10) да поддържа способността за своевременно възстановяване на наличността и достъпа до Личните данни в случай на физически или технически инцидент;
(11) да прилага процес за редовно тестване, оценка и оценяване на ефективността на техническите и организационните мерки за гарантиране на сигурността на обработката на Лични данни;
(12) да следи за спазването на изискванията на постоянна основа;
(13) прилага мерки за идентифициране на уязвимостите по отношение на обработката на Лични данни в системите, използвани за предоставяне на Услугите;
(14) осигуряване на обучение на служителите и подизпълнителите, за да се гарантира постоянният капацитет за изпълнение на мерките за сигурност, установени в настоящата Документация.
(15) да поддържа регистър на всички категории дейности по обработването, извършени от името на Администратора.

Чл. 5. По отношение автоматичното обработване на Лични данни, ако е приложимо, във връзка с обработката на Лични данни, която се извършва съгласно настоящата Документация, Обработващият:

(1) определя помещения, в които да се разположат елементите на комуникационно-информационните системи за обработване на Личните данни;
(2) гарантира, че системите за автоматично обработване на Лични данни се използват само от упълномощени лица;
(3) гарантира, че лицата, оправомощени да използват системи за автоматично обработване на Лични данни, имат достъп само до Личните данни, съответстващи на тяхното овластяване и въз основа на конкретни разрешения, дадени нарочно за тези лица;
(4) предотвратява неоторизиран достъп до носители на Данни.

Чл. 6. Обработващият лични данни предприема разумни мерки, за да гарантира, че няма да назначи лице, което да обработва Лични данни, освен ако това лице:

02-992 40 58

office@gglaw.bg
www.gglaw.bg

гр. София 1000,
ул. Цар Шишман №3, ет.1
„Господинов и Генчев“

(1) е компетентно и квалифицирано да изпълнява конкретните задачи, възложени му от Обработващия;
(2) е било упълномощено от Обработващия;
(3) е било инструктирано от Обработващия относно изискванията, свързани с изпълнението на задълженията на Обработващия лични данни съгласно тези клаузи, и по-специално относно ограничената цел на обработката на данни.

Чл. 7. Персоналът на Обработващия данните е длъжен да се държи по начин, съответстващ на насоките на Обработващия по отношение на поверителността, бизнес етиката, подходящата употреба и професионалните стандарти. Обработващият данните извършва разумно подходящи проверки на миналото, доколкото това е законово допустимо и в съответствие с приложимото местно трудово законодателство и законови разпоредби.

Чл. 8. Обработващият може да прави периодични тестове или симулации, за да се види дали персоналът е запознат с техните отговорности спрямо защитата на Личните данни. Вследствие на това трябва да се осигури целенасочено обучение за тези лица от персонала, които не успеят да се справят с теста.

Чл. 9. Обработващият данни използва географски разпределени центрове за данни и съхранява всички Лични данни във физически защитени центрове.

Чл. 10. Обработващият поддържа физически стандарти за сигурност, предназначени да забранят и недопуснат неоторизиран физически достъп до помещенията и оборудването на Обработващия, в което се извършва обработката на Личните данни, предмет на настоящата Документация, в това число:

(1) определя помещенията, в които ще обработват Личните данни;
(2) определя и въвежда контрол на зоните за сигурност чрез подходящ контрол за влизане, за да се гарантира че достъп имат само оторизирани лица;
(3) осъществява видеонаблюдение на достъпа до помещенията, включително на забранените зони и оборудването в помещенията;

Чл. 11. Помещенията са проектирани така, че да издържат на неблагоприятни метеорологични условия и други разумно предвидими природни условия, защитени са от денонощна охрана, видеонаблюдение, проверка на достъпа и контролиран от ескорт достъп, а също така се поддържат от резервни генератори на място в случай на прекъсване на електрозахранването.

Чл. 12. Електрозахранващите системи на центровете за данни са проектирани така, че да са резервирани и да могат да се поддържат без въздействие върху непрекъснатите операции 24 часа в денонощието, 7 дни в седмицата.

Чл. 13. В повечето случаи за критичните инфраструктурни компоненти в центъра за данни е осигурен както основен, така и алтернативен източник на захранване.

02-992 40 58

office@gglaw.bg
www.gglaw.bg

гр. София 1000,
ул. Цар Шишман №3, ет.1
„Господинов и Генчев“

Чл. 14. Резервното захранване се осигурява от различни механизми, като например батерии на непрекъсваеми захранващи устройства (UPS) или дизелови генератори, които са в състояние да осигурят аварийно електрозахранване или надеждна защита на захранването при прекъсвания на електроснабдяването, спиране на тока, свръхнапрежение, поднапрежение и условия на непоносима честота.

Чл. 15. Инфраструктурните системи са проектирани така, че да елиминират единичните точки на повреда и да сведат до минимум въздействието на очакваните екологични рискове.

(4) Производственото оборудване и съоръженията на подпроцесора на данни имат документирани процедури за превантивна поддръжка, в които подробно е описан процесът и честотата на извършване в съответствие с изискванията на Администратора или вътрешните спецификации.

(1) Превантивната и коригиращата поддръжка на оборудването на центъра за данни се планира чрез стандартен процес на промяна в съответствие с документираните процедури.

Чл. 16. Обработващият поддържа следните правила, политики, стандарти и процедури за контрол на достъпа и администриране на съответната ИТ среда, ако е приложимо, във връзка с обработката на данни, които се извършват съгласно настоящата Документация:

(1) приема се политика за контрол на достъпа, която документира подходящи практики в областта на търговската и информационната сигурност, която политика следва да включва и следното: поставяне на ключалки на шкафове и сейфове, в които се съхраняват на хартия лични данни, поставяне и осигуряване функционирането на пожарогасителни средства;

(2) приемане на формален процес на регистрация и дерегистрация на потребители, който се прилага с оглед възлагането на права за достъп;

(3) приемане на формален процес за достъп на потребители, който се прилага при възлагане или оттегляне на права за достъп за всички видове потребители до всички видове системи и услуги;

(4) приемане на формален процес за управление и контролирано предоставяне на информация за тайна идентификация;

Чл. 17. Правата за достъп на потребителите се преразглеждат на редовни интервали от време.

(1) достъпът до системи и приложения за обработване на лични данни се контролира чрез подходяща и сигурна процедура за регистрация и вписване;

02-992 40 58

office@gglaw.bg
www.gglaw.bg

гр. София 1000,
ул. Цар Шишман №3, ет.1
„Господинов и Генчев“

(2) администраторските профили следва да се използват само за целта за изпълнение на административни дейности;

(3) достъпът до компютри и сървъри трябва да бъде според и в съответствие с обхвата на длъжността и функциите на служителя или изпълнителя.

(4) броят на хранилищата на лични данни (бази данни, файлове, копия, архиви) трябва да се държи на абсолютния минимум като се избягва ненужно дублиране. Вместо дублиране, трябва да се предпочитат псевдонимизирани бази данни, които претърсват главните хранилища за конкретни лични данни, ако и когато е необходимо.

Чл. 18. Обработващият се задължава да осигури възможност да възстанови своевременно наличността и достъпа до Личните данни в случай на физически или технически инцидент:

(1) за всички системи, обработващи Лични данни, са установени изисквания за непрекъсваемост на работата и са изготвени и тествани планове за възстановяване след инцидент.

Чл. 19. Обработващият използва логическа изолация, за да отдели Личните данни на всеки Субект на данни от тези на другите. Това осигурява мащаб, като в същото време стриктно предотвратява неоторизиран достъп до Личните данни на Субект на данните.

Чл. 20. На Администратора се предоставя контрол върху специфичните средства за контрол за споделяне на достъпа до данните на Субектите на данни за конкретни цели в съответствие с функционалността на Услугите.

Чл. 21. Директният достъп до Данните на Субекта на данните е ограничен и в случай че такъв е необходим, се установяват и прилагат права на достъп само за надлежно упълномощен персонал в допълнение към правилата за контрол на достъпа, посочени в настоящия раздел.

Чл. 22. Конфигурациите на защитната стена и маршрутизатора трябва да се настроят така, че да се ограничи входящия и изходящия трафик от “ненадеждни” мрежи (включително безжични) и хостове. Забранете целия друг трафик, освен този за протоколите, необходими за средата за личните данни (PDE).

Чл. 23. Трябва да се прилагат засилено криптиране и протоколи за сигурност, за да се защитят личните данни по време на предаването през отворени, обществени или ненадеждни мрежи.

Чл. 24. Трябва да се използват инструменти за сигурност, за да се следи и контролира потока на лични данни през крайните точки и към външни мрежи.

Чл. 25. Инструкции или стандарти за сигурност трябва да бъдат разработени и приложени за бази данни, приложения, операционни системи и приложения, съдържащи Лични данни.

02-992 40 58

office@gglaw.bg
www.gglaw.bg

гр. София 1000,
ул. Цар Шишман №3, ет.1
„Господинов и Генчев“

Чл. 26. Периодът за запазване на Личните данни трябва да бъде ограничено до времето, необходимо за всяка отделна обработваща дейност, макар и в съответствие със законовите и/или регулаторните задължения.

Чл. 27. Паролите за системите и устройствата, управляващи Лични данни, трябва да съдържат най-малко 8 символи и съдържат знаци от три от следните пет категории:

(1) Английски главни букви (от A до Z)
(2) Английски малки букви (от a до z)
(3) Цифри (0 до 9)
(4) Небуквени символи (например: !, $)
(5) Който и да е Уникод знак, непопадащ в предходните четири категории. Последната пета категория може да варира по регион.

Чл. 28. Паролите не трябва да се приписват лесно на Субекта на данни и те трябва да се променят поне на всеки 3 месеца.

Чл. 29. Системните ресурси и правото на достъп трябва да бъдат зададени по потребителски акаунти, а потребителските акаунти да бъдат зададени на уникални потребители.

Чл. 30. Отдаленият достъп (от външни мрежи) трябва да бъде защитен чрез многофакторна автентикация.

Чл. 31. Видимостта на Личните данни трябва да бъде ограничена до единствения набор от Лични данни, които са необходими за отделните дейности по обработка. На Обработващия не трябва да се предоставят Лични данни, които не са му нужни.

Чл. 32. Достъпът до продуктови среди, съдържащи Лични данни, и когато е технически възможен - достъпът до Лични данни, трябва да бъде наблюдаван и регистриран, за да се установи точно връзката между достъпа и лицето, което достъпва Личните данни. Логовете трябва да бъдат защитени от подправяне.

Чл. 33. Записват се най-малко следните записи в регистъра на одита за всички системни компоненти, обработващи лични данни, за всяко събитие:

(1) Идентификация на Потребителя
(2) Вид събитие
(3) Дата и час
(4) Индикация за успех или неуспех
(5) Източник на събитието
(6) Идентификация на засегнатите данни, системен компонент или ресурс.

Чл. 34. Във връзка със задължението за уведомяване, Обработващият се задължава да се създаде и поддържа регистър на нарушенията на Личните данни.

GG LAW
WE CARE FOR YOUR SUCCESS

02-992 40 58

office@gglaw.bg
www.gglaw.bg

гр. София 1000,
ул. Цар Шишман №3, ет.1
„Господинов и Генчев“

GG LAW
WE CARE FOR YOUR SUCCESS

02-992 40 58

office@gglaw.bg
www.gglaw.bg

гр. София 1000,
ул. Цар Шишман №3, ет.1
„Господинов и Генчев“

ПРИЛОЖЕНИЕ III КЪМ ДОКУМЕНТАЦИЯ ЗА ЗАЩИТА НА ДАННИТЕ ОТ „ОДО ПРО“ ООД

III. ПОДИЗПЪЛНИТЕЛИ

Чл. 1. Администраторът потвърждава и се съгласява, че:

(7) Партньорите на Обработващия могат да бъдат наети като Подизпълнители; и
(8) Обработващият и съответно партньорите на Обработващия могат да ангажират Подизпълнители във връзка с предоставянето на Услугите.

Чл. 2. В случай на използване на Подизпълнители, Обработващият изисква от тях да спазват разпоредбите на настоящата Документация и гарантира, че Администраторът може също така да упражни своите права, произтичащи от настоящата Документация, директно върху такива Подизпълнители.

Чл. 3. В случай, че е планирано използване на Подизпълнители от трета държава (извън ЕС и/или ЕИП), Обработващият гарантира, че съответните Подизпълнители поддържат подходящо ниво на защита на данните (например чрез сключване на споразумение, основано на стандартните договорни клаузи на ЕС). Обработващият ще предостави на Администратора доказателства за съществуването на такива споразумения с Подизпълнителите по искане на Администратора.

Чл. 4. Администраторът може писмено да оспори включването на даден Подизпълнител, като за целта предостави обективни причини за това. Оспорването се разглежда от Обработващия и на Администратора се представя писмено становище за предприетите мерки.

Чл. 5. При включване на Подизпълнител в обработката, Обработващият ще отговаря пред Администратова за изпълнение на задълженията на включения Подизпълнител.

Чл. 6. Списъкът на Подизпълнителите на Обработващия може да бъде разкрит при изрично писмено поискване.