

ОБЩА ПОЛИТИКА ЗА ЗАЩИТА НА ЛИЧНИТЕ ДАННИ

Тази Политика съдържа правила, които „ЕлЕлКлауд” ООД, с ЕИК 206851771 е задължено да спазва ежедневно, с оглед изискванията на приложимото законодателство относно защитата на личните данни, включително Общия регламент за личните данни (GDPR).

2021 г.

Въведение

Настоящата Обща политика за защита на личните данни („**Политика**“) се използва от „ЕлЕлКлауд“ ООД (наричано по-долу „**ЕЛЕЛКЛАУД**“ или „**Дружеството**“), в съответствие с Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (GDPR) („**Общия регламент за личните данни**“ или само „**Регламента**“) и при отчитане разпоредбите на останалото приложимо законодателство за защита на личните данни.

Използваните в този документ думи „**ние**“, „**нашия**“ и други подобни се отнасят за „ЕлЕлКлауд“ ООД, освен ако друго не следва от контекста.

Относно значението на използваните в този документ термини с начална главна буква и абревиатури моля вижте в раздел „Дефиниции“ накрая на този документ.

Значение на защитата на личните данни за нас

Личната неприкосновеност на нашия екип, клиенти, партньори, контрагенти и други физически лица, на които ЕЛЕЛКЛАУД обработва лични данни в процеса на осъществяване на дейността си, е изключително важна за нас. Защитата на личните данни на тези лица и използването им по добросъвестен и законосъобразен начин е от огромно значение за ценностите на ЕЛЕЛКЛАУД и е определящ елемент от поддържането на отношенията ни с нашите клиенти и партньори, и за нашата репутация.

Цел на Политиката

Тази Политика цели да улесни практическото прилагане на законодателството по защита на личните данни от Дружеството и нашия Екип, като описва принципите и процедурите, които ЕЛЕЛКЛАУД се е ангажирал да спазва, с цел да осъществява дейността си в съответствие със законодателството за личните данни, както и отговорностите на нашия екип при обработване на лични данни.

Политиката е насочена към предотвратяване на незаконното или недобросъвестно обработване на лични данни (например неоторизирано разкриване, съхранение, промяна или унищожение на лични данни).

Обхват

Тази Политика е част от вътрешните правила и процедури на ЕЛЕЛКЛАУД и се отнася за всички лични данни обработвани от Дружеството: както лични данни, обработвани (а) изцяло или частично с автоматични средства, така и (б) на хартиен носител.

Политиката се прилага към Управителя на ЕЛЕЛКЛАУД, както и към екипа на ЕЛЕЛКЛАУД (които, за целите на настоящите Правила, включват и лицата, работещи за Дружеството по трудови и граждански договори (наричани общо „**екип**“)). Екипът има задължението да се запознае с, осмисли и да спазва тази Политика при изпълнение на функциите си за Дружеството. Управителят на ЕЛЕЛКЛАУД е отговорен за прилагането на Политиката в дейността на ЕЛЕЛКЛАУД и за осигуряване нейното спазване, както и на законодателството за личните данни, от целия екип.

Умишленото или по непредпазливост неспазване на тази Политика и други вътрешни правила относно обработването на лични данни и законодателството за личните данни от служители на дружеството или лица, работещи за него по договори, приравнени на трудовите представлява нарушение на трудовата дисциплина и е основание за предприемане на предвидените дисциплинарни мерки от страна на ЕЛЕЛКЛАУД в съответствие с Кодекса на труда. В допълнение, нарушението на правилата относно защита на личните данни от съответните служители в определени случаи може да доведе и до търсене на наказателна отговорност.

Тази Политика се спазва едновременно с приложимото законодателство за личните данни, като последното има приоритет пред Политиката в случай на противоречие или когато законодателството за личните данни предвижда по-строги правила.

Ако законодателството за личните данни изисква преглед на тази Политика, то тя ще се преглежда и актуализира съответно.

Принципи на защита на личните данни

Ние от ЕЛЕЛКЛАУД заявяваме, че ще направим всичко необходимо, за да спазваме задълженията си, произтичащи от законодателството за личните данни и ще съобразяваме изцяло дейността си с долуизброените принципи и други основни нормативни изисквания относно защитата на личните данни (наричани заедно „Принципи“).

Принцип 1: Законсъобразност

Ние ще обработваме лични данни само, ако имаме *законно основание*, определено в законодателството за личните данни. Ние обработваме лични данни на законно основание, когато това обработване е необходимо за:

- нашия (или на трето лице) **легитимен бизнес интерес**: например наш легитимен интерес е осъществяване на тестове, за което сме се задължили по договор с наш клиент. Ние обаче не можем да разчитаме на основанието легитимен интерес, когато пред този интерес преимущество имат интересите или основните права и свободи на Субектите на обработваните данни и особено когато Субектът на данните е дете;
- спазване на **наше правно задължение** (напр. за целите на данъчното облагане или за уведомяване на съответните държавни органи при възникнал инцидент) или
- **изпълнението на договор**, който сме сключили със Субекта на данните, както и за предприемане на действия по искане на Субекта преди сключването на договор (напр. за да осъществим тест следва да разполагаме с имената на лицето, което ще осъществява теста).

Обработването на лични данни се извършва със **съгласието** на съответния Субект, в много краен случай и доколкото може да се окаже неосъществимо получаване на валидно съгласие поради по-строгите изисквания по Регламента, по изключение е възможно да обработваме лични данни на някое от горепосочените основания, когато това е възможно. Съгласие обаче ще е необходимо за използването на „бисквитки“ и подобни технологии на интернет страниците на Дружеството, за регистриране на потребителски профил при качване или сваляне на данни при извършване на тестове и т.н.

ВАЖНО:

- Всеки член на нашия екип следва да се увери, че е налице законно основание за всяко обработване на лични данни, за които е отговорен.
- Ако се налага да бъдат поискани допълнителни лични данни или да се промени начинът на обработване на лични данни, ние следва винаги да проверим дали е налице законно основание за това.
- В случай, че лични данни са предоставени от Субект на данни на ЕЛЕЛКЛАУД без правно основание по чл. 6, параграф 1 от Регламента или в противоречие с принципите по чл. 5 от същия регламент, в срок един месец от узнаването ЕЛЕЛКЛАУД е задължен да ги върне, а ако това е невъзможно или изисква несъразмерно големи усилия – да ги изтрие или унищожи. Изтриването и унищожаването се документират с протокол на Управителя.
- ЕЛЕЛКЛАУД може да копира документ за самоличност, свидетелство за управление на моторно превозно средство или документ за пребиваване, само ако това е предвидено със закон. Във всички случаи, когато копирането на посочените документи не е нормативно предвидено, ЕЛЕЛКЛАУД може да ги изисква от Субектите на лични данни единствено с цел да провери самоличността им и точността на изписването на личните им данни, ако възникне такава необходимост, и да им ги върне обратно, без да ги копира или сканира.
- ЕЛЕЛКЛАУД не предоставя свободен публичен достъп до информация, съдържаща единен граждански номер или личен номер на чужденец.
- ЕЛЕЛКЛАУД предприема подходящи технически и организационни мерки, които не позволяват единният граждански номер или личният номер на чужденец да е единственото средство за идентификация на потребителя при предоставяне на отдалечен достъп до съответната електронна услуга. Например, лица, които желаят да се логнат в системата на LLcloud, се регистрират на само с въвеждането на user name или имейл, и парола, а ЕЛЕЛКЛАУД не изисква и не събира по никакъв начин ЕГН или ЛНЧ от тях.

Принцип 2: Добросъвестност и прозрачност

За да бъдем добросъвестни и прозрачни в действията си по обработване на лични данни, ние трябва да обясним открито на физическите лица как обработваме техните данни, по ясен и достъпен за тях начин, използвайки обикновен език (без използване на специални термини, доколкото е възможно). Тази информация следва да включва какви лични данни събираме, как възнамеряваме да ги използваме, с кого можем да ги споделим, ако възнамеряваме да ги трансферираме в страни извън Европейското икономическо пространство („ЕИП“), както и как лицата могат да се свържат със ЕЛЕЛКЛАУД за въпроси или за упражняване на техни права.

Ние предоставяме горепосочената информация на нашите клиенти, желаещи да участват в тестове лица и служители посредством документ, наречен *Уведомление за поверителност*, а на посетителите на нашата интернет страници, и чрез нашата *Политика относно „бисквитките“*.

ВАЖНО:

- Ако е необходимо да изискваме допълнителни лични данни или да променим начина на обработване на лични данни, ние винаги ще съобщаваме дали следва да се

предостави допълнителна информация на съответните Субекти. Особено внимание следва да се обърне върху информирането на физическите лица относно използване на техни данни за цели, които лицата не очакват.

Принцип 3: Ограничение на целите

Лични данни могат да се използват само за целите, за които данните са събрани. Ние не следва да използваме лични данни за цели, за които физическото лице не е уведомено или които не са очевидни за лицето (или не са съвместими с първоначалната цел). Например:

- служителът следва единствено да разкрива лични данни на други лица единствено когато тези други лица е необходимо да разполагат с тях за изпълнение на тяхната функция или задача, т.е. когато лицето следва да разполага с въпросните данни, за да си изпълнява задачите;
- за да определи дали новата цел на обработване е съвместима с първоначалната цел, за която са събрани данните, екипът следва да прецени дали е налице връзка между тези цели, обстоятелствата, при които лични данни са събрани и отношенията между лицата, естеството на личните данни, възможните последици от бъдещото обработване на данните и потенциалните мерки за сигурност;

Принцип 4: Свеждане на данните до минимум

Личните данни, които ние събираме, трябва да бъдат относими и ограничени до минимално необходимото за целите, за които данните се събират. Ние няма да искаме повече лични данни отколкото имаме нужда с оглед на закономото основание, на база на което ги събираме. Ние ще извършваме проверки относно относимостта на личните данни, които се събират от нашия Екип, за да осигурим съобразяването на настоящия принцип в дейността на ЕЛЕЛКЛАУД.

Ние съобразяваме следните техники на свеждане на данните до минимум, когато използването им е възможно и целесъобразно:

- **По-малкото е повече:** ние винаги следва да си задаваме въпроса: дали се нуждаем да събираме тази информация за постигане на целите ни? Пример за прекомерно събиране на лични данни е изпращането на общ въпросник до желаещи да тестват сензор и софтуер за него, който въпросник включва конкретни въпроси за семейството и/или работа на кандидата, без да е необходима тази информация за конкретния случай за преценка на кандидата.
- **Псевдонимизация:** означава обработване на лични данни по такъв начин, че данните не могат повече да бъдат свързани с конкретен Субект, без да се използва допълнителна информация, при условие че допълнителната информация се съхранява отделно и са взети технически и организационни мерки за осигуряване, че данните не са свързани с конкретно физическо лице. Пример: в определена база данни идентификаторът име и ЕГН са заменени с код, като информацията за това на кой код кое име/ЕГН съответства се съхранява отделно.

Принцип 5: Точност на данните

личните данни следва да бъдат точни и актуални. Ние ще приканваме физическите лица да ни информират за всякакви промени в техните лични данни (и съответно ще актуализираме, поправяме или изтриваме нашите записи).

ВАЖНО:

- Ние не следва да използваме лични данни, за които има съмнение, че не са актуални, без да потвърди тяхната точност.
- Ние трябва да осигурим точното записване и управление на личните данни в съответните системи. Неотнoсима или остаряла информация следва да се премахва и унищожаване в съответствие с нашата *Политика относно съхранение и унищожаване на документи и информация, съдържащи лични данни*.
- Ако бъдем уведомени за промяна в данни на клиент или друг наш контрагент, съответната база данни следва да бъде актуализирана без отлагане.

Принцип 6: Ограничение на съхранението

лични данни не следва да се съхраняват по-дълго, отколкото е нужно за осъществяване на законосъобразната цел, за която те са събрани. След постигането на целта, данните следва да бъдат унищожени по сигурен начин. Това принципно изискване търпи корекция с оглед на разпоредбите на други закони, които налагат да задържим информация за по-дълго време и в определени случаи, нашия легитимен интерес. За повече подробности се съдържат в *Политика относно съхранение и унищожаване на документи и информация, съдържащи лични данни*.

Ако личните данни не могат по някаква причина да бъдат унищожени или заличени (или анонимизирани), настоящият принцип ще бъде спазен, ако информацията е „извадена от употреба“, при условието, че ние:

- не сме в състояние или няма да правим опити да използваме личните данни за взимане на решения, които се отнасят за Субекта на данните или по друг начин, които засяга Субекта;
- ограничаваме достъпа до личните данни с подходящи технически и организационни мерки; и
- се ангажираме да извършим окончателно унищожение на данните по сигурен начин, ако и когато това стане възможно.

Принцип 7: Цялостност и конфиденциалност на данните

личните данни следва да бъдат съхранявани и използвани по сигурен начин. Необходимо е данните да бъдат защитени срещу неразрешено или незаконно обработване и срещу случайна загуба, повреда или унищожаване. Това се прилага по отношение на нашите информационни системи, интернет страници и ежедневното обработване на данни, което ние извършваме. Като минимум, ние ще се съобразяваме с всякакви мерки за сигурност, изисквани от закона.

Някои от мерките за сигурност, които сме предприели, включват: предотвратяване загуба на данни; правила за пароли; анти-малуеър; други.

Определяне на обработващи на данни

Ако ЕЛЕЛКЛАУД (в качеството ни на администратор) ангажира друга организация да обработва лични данни за наша сметка, тази друга организация (“обработващ данни”) трябва да е приложила “подходящи технически и организационни мерки” да отговори на изискванията на приложимото законодателство за личните данни и да осигури защитата на

правата на физическите лица. Като част от този процес, ние ще сключим писмен договор с обработващия данни с изискуемото от закона съдържание.

В рамките на договореното между ЕЛЕЛКЛАУД и обработващите данни съгласно чл. 28 от Регламента, ние ще извършваме прегледи на своите обработващи (и евентуално на обработващи подизпълнители), по-конкретно на техните системи, регистри, помещения, екип и други ресурси, свързани с предоставяне на съответните услуги, с цел да се уверим, че обработващите спазват договорните си задължения и приложимите законодателство за защита на данни.

Принцип 8: Трансфери на данни извън ЕИП

Законодателството за личните данни ограничава трансферите на лични данни извън ЕИП (включително и към дружества в качеството им на обработващи данни) освен когато е налице достатъчна защита на личните данни или са предприети предписани мерки за осигуряване защитата на данните. ЕЛЕЛКЛАУД може в редки случаи да трансферира данни на други лица извън ЕИП, което ние ще извършваме в съответствие с одобрени от ЕК стандартни договорни клаузи, регулиращи трансферите на определени данни между нас и други дружества.

В ограничен брой други случаи лични данни също могат да бъдат трансферирани извън ЕИП, а именно когато:

- данните са изпращани в държава или на международна организация, които са признати от Европейската Комисия (ЕК) като прилагайки адекватни мерки за защита (включват се и американски организации, които са сертифицирани по *Щита за личните данни в отношенията ЕС - САЩ*);
- се разчита на обвързващи корпоративни правила;
- се разчита на стандартни клаузи за защита на данните, приети или одобрени от Европейската Комисия;
- субектът е дал изрично съгласие за трансфера;
- това е необходимо за изпълнение на договор между субекта на данните и ЕЛЕЛКЛАУД;
- се налага по причини от важен обществен интерес; или
- се налага за завеждане, упражняване или защита от правна претенция.

Принцип 9: Зачитане на индивидуалните права на Субектите на данни

Ние винаги ще зачитаме правата на физическите лица, предоставени им със законодателството относно личните данни, включително (и доколкото е приложимо):

- да им бъде предоставяна информация за това как техните лични данни се обработват (вижте за повече подробности *Принцип 2: Добросъвестност и прозрачност по-горе*);
- да допълваме и коригираме личните данни;
- при поискване, да изтриваме данни или да ограничаваме обработването;
- при поискване, да трансферираме лични данни на друг администратор;

- правото им да възразяват срещу обработване, основано на легитимен интерес на ЕЛЕЛКЛАУД или на трета страна или на извършвания по отношение на тях директен маркетинг (включително профилиране, свързано с директен маркетинг);
- да не бъдат обект на изцяло автоматизирани решения (включително профилиране), които пораждаат правни последици или съществено засягат физическите лица.

Ние ще отговорим на всяка молба своевременно и нормално в едномесечен срок от получаването ѝ, така както е предвидено в нашата *Политика относно упражняване на правата на Субектите на данни и отговаряне на искания на трети лица за разкриване на лична информация*.

Принцип 10: Отчетност

Ние ще предприемем широк набор от мерки за намаляване на риска от неговото неспазване и за доказване, че се отнасяме с нужната сериозност към защитата на личните данни. Описание на някои от тези мерки са посочени по-долу.

Регистри за дейностите по Обработка на данни

Преди началото на прилагане на Регламента (25 май 2018 г.) Законът за защита на личните данни изискваше Администраторите да регистрират в КЗЛД своите дейности по обработване на данни. С влизането в действие на Регламента ние сме задължени да поддържаме регистри на извършваното от нас обработване на лични данни, които съдържат описание, наред с друго, на категориите лични данни и основанията за тяхното обработване, определяне на длъжностите, свързани с обработване и защита на данни. Тези регистри следва да бъдат предоставени на КЗЛД при поискване.

Обучение на Екипа

При постъпване на работа в ЕЛЕЛКЛАУД, служителите са задължени да прочетат тази Политика и да декларират, че ще я спазват. Служителите, които обработват лични данни като съществена част от трудовата си функция, ще получат подходящи инструкции и обучение относно защита на данните, както и ще се извършва периодично инструктиране и обучение на Екипа по тези въпроси.

Нови системи и процеси

Законодателството за личните данни изисква от нас да вземаме под внимание и прилагаме мерки за защита на данните в дейностите си по тяхната обработка (известни като Принцип на защита на личните данни на етапа на проектиране (Privacy by Design) и по подразбиране (Privacy by Default).

Ние се придържаме към горепосочения принцип като:

- идентифицираме рисковете за личната неприкосновеност в самото начало на всеки нов проект и преди внедряването на нова система, продукт или услуга, и планиране на действия за тяхното адресиране;
- следваме на принципа за минимизиране на данни, включително прилагане на псевдонимизация на данните, когато е възможно и оправдано от бизнес гледна точка;

- зачитаме личната неприкосновеност при проектирането и употребата на нашите технологии, действия и процеси, и консултиране с всички заинтересовани лица;
- поддържаме високи стандарти на нашите продукти и услуги; и
- се стремим да бъдем прозрачни към физическите лица за това какво правим за защита на техните лични данни.

Оценка на въздействие

През януари 2019 г. ЕЛЕЛКЛАУД е извършило анализ и оценка на нивото на риска върху защитата на личните данни, съгласно който обработването на лични данни от Дружеството, с оглед естеството, обхвата, контекста и целите на обработването няма да породи висок риск за правата и свободите на физическите лица.

Ако обаче в определен момент бъде констатирана вероятност от „висок риск“ при обработването или ЕЛЕЛКЛАУД започне да извършва някоя от операциите по обработване, посочени в публикувания от КЗЛД „Списък на видовете операции по обработване на лични данни, за които се изисква извършване на оценка за въздействие върху защитата на данните съгласно чл. 35, пар. 4 от Регламент (ЕС) 2016/679“¹, съответните операции следва да бъдат подложени на по-задълбочен анализ и оценка (т.нар. „Оценка на въздействието на защитата на данни“) съгласно изискванията на Регламента.

Оценката на въздействието следва да включва описание на дейностите по обработка, възникващите от това рискове и приетите мерки за смекчаване на тези рискове и в частност, гаранции и мерки за сигурност по отношение на защитата на данните и за съобразяване с Регламента. В ограничен брой случаи (например ако Оценката за въздействие покаже висок остатъчен риск за правата и свободите на Субектите) ние може да бъдем длъжни да се консултираме със съответните физически лица или с КЗЛД.

Всеки нов продукт, система или услуга, създадени или закупени от нас, включващ обработване на лични данни, които: (i) не са от вид, обработван досега; или (ii) не са използвани досега по такъв начин; или (iii) обработването на тези данни може да бъде възприети от нашите клиенти, служители или други физически лица като застрашаване на тяхната лична неприкосновеност, следва да бъде анализиран, за да се установи дали това обработване засяга правата и свободите на съответните физически лица и дали обработването следва да се квалифицира като „високорисково“.

Вътрешни одити

Ние ще проверяваме периодично доколко дейността по Обработка на данни са в съответствие с горепосочените принципи и със законодателството за личните данни чрез вътрешни одити. Всички членове на нашия екип ще следва да оказват съдействие при извършването на тези одити.

Съдействие на КЗЛД

При поискване ЕЛЕЛКЛАУД е длъжно да оказва съдействие на КЗЛД при изпълнение на нейните задачи и правомощия. Когато при упражняването на правомощията на КЗЛД, може да

¹ Списъкът е публикуван на уебсайта на КЗЛД - <https://www.cdpd.bg/?p=element&aid=1186>

се наруши задължение на ЕЛЕЛКЛАУД за опазване на професионална тайна или друго задължение за опазване на тайна, произтичащо от закон, ЕЛЕЛКЛАУД отказва предоставяне или достъп само до информацията, защитена като тайна.

Задължения и отговорности на Екипа

Членовете на нашите екип имат следните задължения във връзка със защитата на личните данни:

- (1) да са запознати с настоящите Политики и останалите вътрешни актове на ЕЛЕЛКЛАУД, касаещи защитата на лични данни, включително вътрешни указания и инструкции;
- (2) да участват в инструктажи и обучения относно защитата на лични данни, организирани от Дружеството;
- (3) да пазят в конфиденциалност личните данни, до които имат достъп или са им станали известни при или по повод изпълнение на задължения им и да не ги разкриват на неоправомощени трети лица, в това число членове на семейството, приятели и познати, други служители на администратора, за което в договорите с всички членове на екипа се включва клауза за конфиденциалност;
- (4) да не използват лични данни, до които имат достъп при и по повод изпълнение на задълженията си за други цели освен пряко за изпълнение на задължения си; в частност, те нямат право да преглеждат и копират хартиени документи и файлове на компютър или друг електронен носител, за които нямат оторизиран достъп;
- (5) да обработват само лични данни, необходими за изпълнение на конкретните им трудови задължения;
- (6) да уведомяват управителя на ЕЛЕЛКЛАУД при всеки случай на нарушение на сигурността на личните данни, както и при установяване на потенциален риск от такова нарушение;
- (7) да спазват законодателството за личните данни, тази Политика и другите наши вътрешни актове в областта на защита на личните данни;
- (8) уведомяват управителя на ЕЛЕЛКЛАУД прекия си ръководител и ДЛЗД, в случаите когато се налага да обработват лични данни за цели, различни от първоначално определените цели.

Видеонаблюдение

ЕЛЕЛКЛАУД има легитимен интерес да осигури сигурността на всички участници в тестове, което и понякога може да е необходимо условие за извършване на самите тестове и част от тях. За тази цел Дружеството може в редки случаи да извършва видеонаблюдение в публични зони чрез поставяне на видеокамери на лицата, извършващи тестовете. Използването на видеокамери е оповестено чрез поставяне на предупредителни табели на лицата, които използват и носят тези камери и така извършваното видеонаблюдение е афиширано чрез лицата, които го упражняват.

Повече информация относно осъществяването от Дружеството видеонаблюдение ще намерите в нашата *Политика за контрола на видеонаблюдението*.

Основни дефиниции

За целите на настоящата Политика, изброените по-долу термини и абривиатури имат следното значение:

„Администратор“	<p>търговско дружество или друго лице, което (самостоятелно или съвместно с други лица) определя целите на обработване на лични данни и начина, по който данните се обработват.</p> <p>Така например ЕЛЕЛКЛАУД е Администратор по отношение на обработваните от него лични данни на членове на неговия екип, клиенти и лица, извършващи тестове.</p>
„законодателство за/относно личните данни“	<p>Регламентът за личните данни и други актове на Европейския съюз относно защитата на личните данни, както и всеки нормативен акт, който имплементира и/или създава мерки за прилагане на тези европейски актове или допълнителна национална уредба относно защитата на лични данни в България (включително ЗЗЛД и Наредба № 1 от 30 януари 2013 г. за минималното ниво на технически и организационни мерки и допустимия вид защита на личните данни, указания и практика на КЗЛД, както и съдебна практика, доколкото са съвместими с Регламента за личните данни), и всеки друг закон или нормативен акт, който изменя, допълва, заменя или консолидира гореизброените актове.</p>
„Дружеството“	е „ЕлЕлКлауд“ ООД, с ЕИК 206851771; наричано още „ЕЛЕЛКЛАУД“.
„ЗЗЛД“	действащия Закон за защита на личните данни (ДВ, бр. 1 от 2002 г., с последващи изменения).
„КЗЛД“	Комисия за защита на личните данни.
„лични данни“ или „данни“	<p>са всяка информация, свързана с идентифицирано физическо лице (служител, клиент, доставчик на услуги) или физическо лице, което може да бъде идентифицирано (а) чрез тази информация или (б) чрез тази информация, разглеждана във връзка с друга информация, която Администраторът притежава или може да придобие.</p> <p>Примери на лични данни са: име, адрес, дата на раждане, номер на банкова сметка, мнения за физическото лице, видеозаписи и аудиозаписи. Анонимната информация не представлява лични данни. Фактът, че определена информация е публично достъпна (напр. чрез LinkedIn) не пречи приложението на законодателството за личните данни спрямо такава информация.</p> <p>Физическото лице може да бъде идентифицирано, пряко или непряко, чрез определен идентификатор като име, ЕГН, местонахождение, онлайн идентификатор или чрез един или повече фактори,</p>

	специфични за физическата, психологическа, генетична, икономическа, културна или социална идентичност на това физическо лице.
„Нарушение на сигурността (на данните)“	означава нарушение на сигурността на личните данни, което води до случайно и/или неправомерно унищожение, загуба, промяна, неправомерен достъп или разкриване на данните, в процеса на тяхното, съхранение, трансфериране или други форми на обработване.
„обработване (на лични данни)“	Има много широк обхват и включва практически всичко, което ние правим с лични данни, включително тяхното придобиване, съхранение, използване по какъвто и да е начин (организиране, структуриране, адаптиране или промяна, извличане, разкриване чрез предаване, разпространяване и др.), както и унищожаване.
„обработващ (лични данни)“	Физическо или юридическо лице, публичен орган или друга структура, която обработва лични данни от името на Администратора. Пример: външна фирма за IT поддръжка, предоставяща услуги на ЕЛЕЛКЛАУД.
„Общ регламент за личните данни“ („Регламент“)	Има значението, посочено в раздел „Въведение“ по-горе.
„Екип“	Има значението, посочено в раздел „Обхват“ по-горе.
„Принципи“	Има значението, посочено в раздел „Принципи за защита на личните данни“ по-горе.
„Субект (на лични данни)“	физическо лице, което е идентифицирано или може да бъде идентифицирано (пряко или непряко) въз основа на всяка информация, която може да бъде възприета като лични данни. Вж. също дефиницията на „лични данни“. Служителите и клиентите на ЕЛЕЛКЛАУД са Субекти (на лични данни).
„Специални категории лични данни“	лични данни, които са обект на специална правна закрила: това са данни разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице (наричани също „Чувствителни данни“). Например информацията за здравословното състояние, който Дружеството съхранява за своя Екип, представлява „Специална категория данни“.

обработването на данни, свързани с осъждания и административни нарушения е допълнително ограничено от приложимите закони и представлява също „Специална категория данни“.

Приложение – Мерки за сигурност

По-долу са посочени някои от мерките за сигурност, които ние от ЕЛЕЛКЛАУД прилагаме по отношение на защита на личните данни.

Физическа защита на данните

Дружеството не извършва дейност в голям офис и на практика не се случва повече от един членовете на екипа се събират много рядко чрез физическо присъствие. По тази причина физическата защита, макар и от основно значение за осигуряване на сигурността на информацията, поради характера на работата на членовете на екипа не е от съществено значение. Практически всеки член на екипа работи сам, физически отделен от другите, дори не в една сграда. Мерки на физическа защита, които ние прилагаме, включват:

- документи, съдържащи лични данни се съхраняват в заключен шкаф или сейф. Ако данните са електронни, те следва да са кодирани, криптирани или защитени с парола, както на хардуерното устройство, така и в мрежа и да им се прави периодически резервно копие (бек-ъп). Ако резервното копие е върху преносимо устройство за съхранение, последното от своя страна следва да се съхранява в заключен шкаф или сейф;
- ненужни копия от хартиени документи и други подобни, съдържащи лични данни, следва да се унищожават със шредер или по друг сигурен начин.

Откриване на данни и Класифициране (*Data Discovery, Cataloging and Classifying*)

В допълнение на горното, ние прилагаме мерки на контрол за гарантиране, че лични данни се обработват по сигурен начин и извън нашите основни системи, включително се защитава информация като:

- копия от бази данни, включващи лични данни, за тестване, анализ и надграждане;
- архиви на електронни пощи, за които е вероятно да съдържат лични данни.

Предотвратяване загуба на данни (*Data Loss Prevention*)

Ние може да използваме като превенция срещу загуба на данни мерки като автоматично блокиране на изходящи мейли и преместване на файлове, съдържащи лични данни, ако те не са били надлежно защитени (напр. чрез криптиране).

В някои ситуации криптиране би могло да бъде автоматично приложени спрямо лични данни, когато такива са идентифицирани и класифицирани в имейл съобщения или прикачени към мейл документи, докато в други случаи съобщенията могат да бъдат сложени под карантина.

Криптиране на данни и имейли

Криптирането е една от няколко техники, изрично упомената в Регламента, като това само по себе си насочва към прилагането ѝ от организациите. В случай на необходимост, ние ще приложим мерки за криптиране на данни, както в статика, така и при използването и изпращането им. Това осигурява, че и при евентуален пробив в някоя от системите ни, информацията ще бъде конфиденциална.

Преносимост на данните

Както посочваме и в Принцип 9 относно индивидуалните права на Субектите, последните имат право да поискат експортване на данни, отнасящи се до тях в подходящ формат, който да може да бъде предоставен на друг доставчик на услуги, който да импортира тези данни с оглед извършване на услуги на Субекта. Макар и упражняването на това право да е с ниска вероятност, ЕЛЕЛКЛАУД използва широкодостъпни продукти (като Microsoft Office) да улесни упражняването на това право.

Облачни услуги по съхранение и споделяне на данни (*Cloud Storage and Sharing Services*)

- ЕЛЕЛКЛАУД ще извършва периодичен преглед на документи, които са предмет на облачни услуги, за да се минимизира споделянето им с външни лица. Трансферите на лични данни, както вътрешно между Екипа, така и извън Дружеството, следва да бъдат извършвани с необходимото внимание и грижа. Така например, когато изпращате имейл, трябва да се уверите, че изпращате информацията на адресата, на когото наистина искате за изплатите имейла, а не на погрешен имейл адрес.
- Имайте предвид, че лицата, търсещи информация, понякога могат да си служат с измамни средства. Преди да изпратите лични данни на трето лице, уверете се в неговата идентичност, особено ако предоставяте информация по телефона. При съмнение, моля обърнете се към управителя на ЕЛЕЛКЛАУД.

Anti-Virus и Anti-Malware

Успешното проникване на вирус или malware (зловреден софтуер) в компютърните системи може да ги направи неизползваеми, но още по-сериозно притеснение от гледна точка на защитата на данните е възможността след такова проникване да бъдат узнати данни относно достъпа на потребителите и администраторските акаунти. По този начин може да бъде получен достъп до лични данни и друга поверителна информация на Дружеството, както съхранявана на негови устройства, така и в облак.

ЕЛЕЛКЛАУД, в тясно сътрудничество с доставчиците на ИТ услуги, полага грижи за осигуряване на практически най-силната защита срещу malware, включително чрез най-актуални анти-вирусни софтуери.

Идентификация на нарушения на сигурността на данните и блокиране (Data Breach Identification and Blocking)

Законодателството за личните данни изисква от нас да уведомяваме без отлагане КЗЛД относно нарушения на сигурността на личните данни (и когато е постижимо, в рамките на 72 часа) след като сме узнали за нарушение на сигурността на лични данни (освен ако нарушението не е вероятно да постави под риск правата и свободите на физическите лица). Ние може също така да трябва да уведомим физическите лица при определени обстоятелства и трябва да документираме нарушенията на сигурността на лични данни в съответствие с нашата *Политика за действие при нарушение на сигурността на данните*.

- Ако член на нашия екип узнае за случай на нарушение на сигурността на лични данни, той следва незабавно да уведоми управителя на ЕЛЕЛКЛАУД и да му предостави цялата информация, с която разполага за случая (включително за естеството и последиците от нарушението и евентуалните мерки, взети или които се предлагат да бъдат взети за редуциране на негативните последици). Примери за нарушения на сигурността на данните са: погрешното изпращане на лични данни на друг адресат, а не на този, който следва да ги получи; осъществен неоторизиран достъп до лични данни; кражба или загуба на документи или мобилни устройства (лаптопи, външна памет и пр.), които съдържат лични данни.

Контакти

Управител на ЕЛЕЛКЛАУД („ЕлЕлКлауд” ООД)

Ставри Николов

stavri.nikolov@llcloud.eu

Технически екип на ЕЛЕЛКЛАУД („ЕлЕлКлауд” ООД)

team@llcloud.eu