Политика за установяване, ескалация и докладване на нарушения в

„АЛУМИНА ЕЛИТ 2003" ЕООД

I. ОСНОВНИ ПОЛОЖЕНИЯ

„АЛУМИНА ЕЛИТ 2003" ЕООД, ЕИК **104612589** , е със седалище и адрес на управление: гр. Велико Търново, кв. Чолаковци, местност Дълга Лъка, представлявано от управителя Диан Атанасов Палазов.

Настоящата политика е част от мерките, целящи осигуряване на информационна сигурност и ефективна система за защита на личните данни в **„АЛУМИНА ЕЛИТ 2003" ЕООД**, които да бъдат в съответствие с действащото законодателство и приложимите добри практики.

Регламент (ЕС) 2016/679 на ЕП 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, който започва да се прилага от 25 май 2018г., както и настоящия Закон за защита на личните данни, поставят фокус върху сигурността на личните данни. С помощта на подходящи технически и организационни мерки данните следва да се обработват по начин, гарантиращ подходяща сигурност, включително защита срещу неразрешена или неправомерна обработка и срещу случайна загуба, унищожаване или вреди. Вредите могат да бъдат както физически, така и материални или нематериални вреди за физическите лица, например загуба на контрол върху личните им данни или ограничаване на правата им, дискриминация, кражба на самоличност или измама с фалшива самоличност, финансови загуби, неразрешено премахване на псевдонимизацията, накърняване на репутацията, нарушаване на поверителността на лични данни, защитени от професионална тайна, или всякакви други значителни икономически или социални неблагоприятни последствия за засегнатите физически лица.

Настоящата политика цели да създаде следните организационни предпоставки:

- даващи ниво на сигурност, съответстващо на риска, възникващ при конкретното обработване на лични данни;
- отчитащи достиженията на техническия прогрес, разходите за прилагане, естеството, обхватът, контекстът и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица;
- осигуряващи своевременно установяване на нарушения в сигурността, необходимост от уведомяване и съответно уведомяване на надзорния орган/ засегнатите субекти на данни.
- при разработването на ефективен план за действие (playbook) за всеки конкретен случай ще се отдава необходимото внимание на всички обстоятелства, свързани с нарушението.

II. КЛЮЧОВИ ПОНЯТИЯ

"Политиката" - настоящата политика за установяване, ескалация и уведомяване за нарушаване сигурността на личните данни, приета от **„АЛУМИНА ЕЛИТ 2003" ЕООД**;

"ОРЗЛД" - Регламент (ЕС) 2016/679 на ЕП 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;

"ЗЗЛД" - Закон за защита на личните данни;

"КЗЛД" - Комисия за защита на личните данни;

"Лични данни" - всяка информация, свързана с идентифицирано физическо лице/физическо лице, което може да бъде идентифицирано. Физическо лице може да бъде идентифицирано (пряко или непряко), по-специално чрез идентификатор като име, идентификационен номер, адрес, онлайн идентификатор или по един или повече признаци, специфични за физическата, физиологичната, генетичната, психическата, умствената, икономическата, културната или социална идентичност на това физическо лице;

"Субект" - физическо лице, за което се обработват Лични данни, независимо дали е контрагент на Дружеството, служител или друго лице, чиито данни се обработват от Дружеството;

"Обработване" - всяка операция/ съвкупност от операции, извършвана с Лични данни/ набор от Лични данни чрез автоматични/ други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване;

"Администратор" - лице, което само или съвместно с други определя целите и средствата за обработването на лични данни. Администраторът в случая е Дружеството;

"Обработващ" – физическо (извън служителите на Дружеството) или юридическо лице, което обработва лични данни по възлагане на Дружеството, като стриктно определя целта и средствата на обработката, вкл. е проверено дали лицето отговаря на изискванията на ОРЗЛД;

"Подобработващ" - подизпълнител на избрания Обработващ;

"Служител" - всяко лице, нает от Дружеството по трудов и/или граждански договор, което обработва Лични данни;

"Специални категории лични данни" - данни съгласно чл. 9 от ОРЗЛД, а именно такива, 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;

Данни, свързани с присъди и нарушения – данни, съгласно чл. 10 от ОРЗЛД, обработването на които се извършва само под контрола на КЗЛД;

"Нарушение на сигурността"[1]- събитие, водещо до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до Лични данни, които се предават, разкриват, съхраняват или обработват по друг начин, като:

- "унищожаване" е налице, когато данните вече не съществуват/ не съществуват във формата, в която могат да се ползват от Администратора;
- "загуба" е налице, когато Личните данни съществуват, но Администраторът е загубил контрол/ достъп/ фактическата власт върху тях;
- "неразрешена или незаконна обработка" е налице, когато има разкриване на Личните данни/ достъп до тях на неоторизирани получатели, както и всяка друга форма на обработка, нарушаваща ОРЗЛД, напр. случайно или неправомерно унищожаване, загуба, промяна, неправомерно разкриване, или достъп до предадени, съхранявани или обработвани по друг нерегламентиран начин лични данни.

- "вреди" са всички физически, материални и нематериални вреди, произтичащи от неразрешена, незаконна обработка или загуба.

Нарушенията на сигурността могат да бъдат разделени на три основни групи:

1. Нарушения на поверителността – във връзка с неоторизирано или случайно разкриване на или достъп до лични данни;

2. Нарушения на достъпността – когато настъпи случайна или неоторизирана загуба или достъп до/унищожаване на лични данни;

3. Нарушение на достоверността – при случайно или неоторизирано изменение на личните данни.

Някои нарушения могат да изпълняват едновременно две или три от условията, описани по – горе в 1 до 3 вкл.

"Екип за реакция" е екип, който се сформира при нарушение на сигурността и който координира дейностите по проучване на обстоятелства по евентуално Нарушение на сигурността, извършва действия по анализ, предложения и ограничаване на вредите; предприема план за действие и мерки по ограничаване на вредите и възстановяване на сигурността на информацията. Екипът се състои от членове с познания и опит в информационната сигурност, човешки ресурси и др. и при необходимост е подкрепен от допълнителни служители от други отдели, напр. правен или информационна сигурност.

III. ЦЕЛ НА ПОЛИТИКАТА

Настоящата политика цели да бъде ефективен инструмент за поддържане на сигурността и за предотвратяване на обработване, което е в нарушение на вътрешните правила на **„АЛУМИНА ЕЛИТ 2003″ ЕООД**, на ОРЗЛД и приложимото законодателство в областта на личните данни; както и да утвърди ефективни защитни мерки в случай на нарушаване на сигурността на лични данни с цел овладяване на инциденти по подходящ и навременен начин.

IV. ДЕЙСТВИЯ ПРИ НАРУШЕНИЯ

Дружеството предприема всички възможни стъпки, за да обучи Служителите да разпознават възникването на Нарушения на сигурността, включително риск от настъпване на такива. Служителите следва да получат ясни указания за приоритетния характер на незабавното подаване на сигнал за евентуално Нарушение на сигурността, като и за необходимото последващо съдействие по предоставяне на писмени подробности за инцидента при първа възможност.

Веднъж запознат с настоящата Политика, всеки Служител следва да я прилага приоритетно в дейностите по Обработване на Лични данни от Дружеството. При възникване на съмнение за Нарушение на сигурността, Служителят, който първи установи вероятността от такова събитие незабавно уведомява Управителя, който след преценка на конкретната ситуация, сформира Екип за реакция.

Екипът за реакция незабавно предприема проучване на сигнала за евентуално Нарушение на сигурността, използвайки всички организационни и технически ресурси на Дружеството, както и последващи действия по анализ, предложения и ограничаване на вредите. Изготвя документ за оценката на възможния риск от нарушението и неговите последици, включително защитните мерки, които могат да смекчат ефекта от него и го препраща на Управителя на Дружеството. Въз основа на документа по предходното изречение Управителят взема обосновано решение дали има задължение:

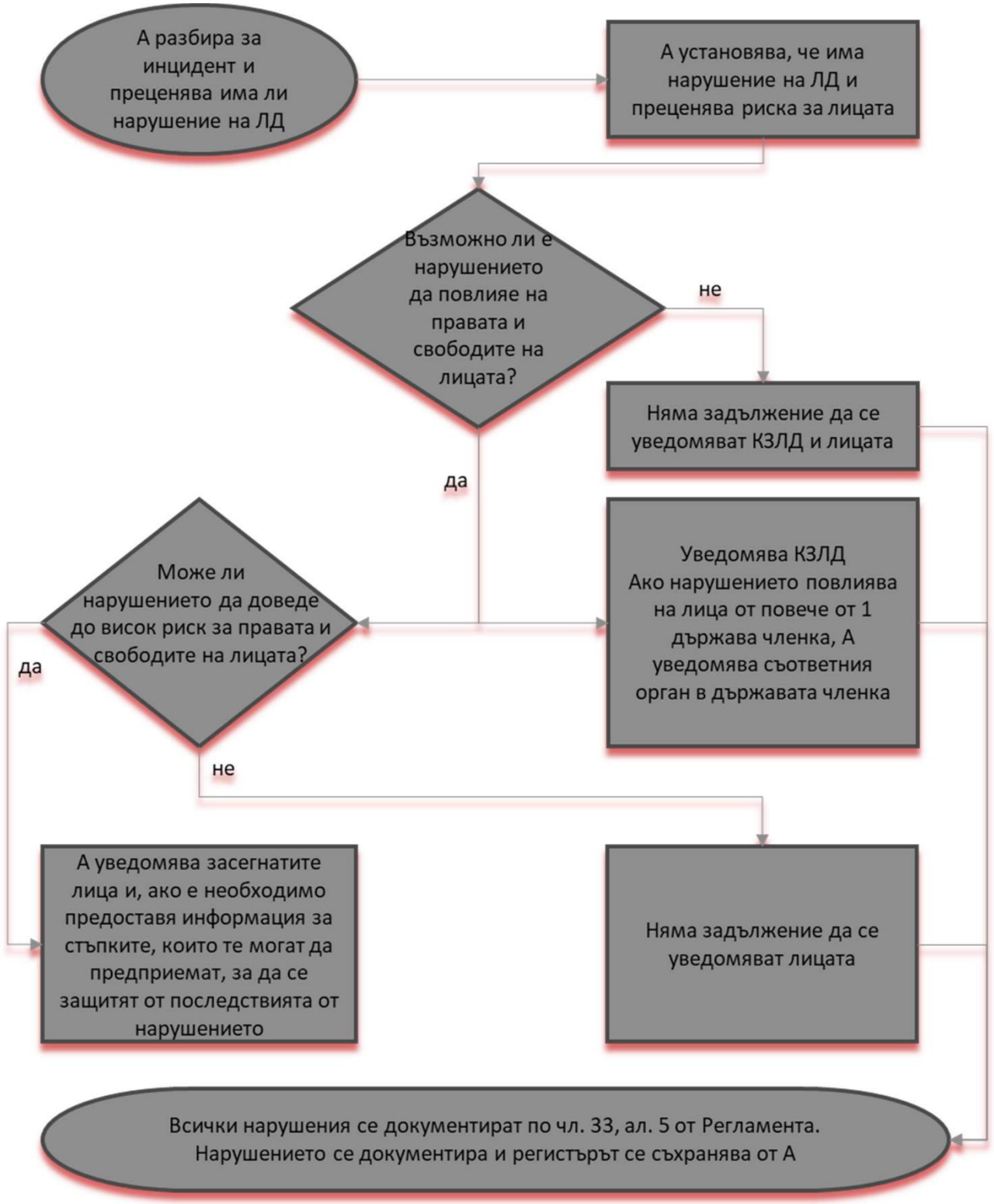
- Да уведоми Комисия по защита на личните данни относно настъпилото нарушение; и

- Да уведоми засегнатите субекти на данни, когато съществува висок риск съгласно предходната точка.

Всяко Нарушение на сигурността подлежи на документиране от Дружеството.

V ПЛАН И УПРАВЛЕНИЕ НА НАРУШЕНИЯТА

Схемата по-долу илюстрира нагледно какви действия следва да бъдат предприети в случай на установено нарушение.



VI. УСТАНОВЯВАНЕ НАРУШЕНИЕ НА СИГУРНОСТТА

На база събраната информация Екипът за реакция оценява риска за субектите в резултат на Нарушението на сигурността. Ако такъв бъде идентифициран, Екипът дава становище по установеното Нарушение на сигурността и препоръчва мерки за минимализиране/ възстановяване вредите.

Когато има вероятност нарушението на сигурността на личните данни да породи висок риск за правата и свободите на физическите лица, Дружеството, в подходящ срок след узнаването и оценката на риска, който може да породи конкретното Нарушение на сигурността, съобщава на субекта на данните за нарушението на сигурността на личните данни.

Уведомлението до засегнатите лица е по утвърден образец. Засегнатите лица следва да бъдат уведомени лично по подходящ начин по преценка на Дружеството - по e-mail, SMS, писмо, по телефона, чрез публично съобщение, така че Субектите да бъдат ефективно информирани.

Условия, при които не е необходимо уведомяване:

- Когато Нарушението на сигурността няма да породи риск за правата и свободите на Субектите на данни;
- Когато Личните данни са публично достъпни и оповестяването им няма да породи риск за Субектите;
- Когато Нарушението на сигурността засяга само поверителността, а засегнатите Лични данни са сигурно шифровани с отговарящ на съвременното технологично равнище алгоритъм, ключът за дешифриране не е разкрит и е генериран така, че да не може да бъде открит с наличните технически средства от лице, нямащо достъп до ключа.

Счита се, че Дружеството е узнало за настъпване Нарушение на сигурността, когато Екипът за реакция даде становище, че са налице предпоставките за възникване на такова.

УВЕДОМЯВАНЕ НА КЗЛД

В срок до 72 (седемдесет и два) часа от узнаване за Нарушението, Дружеството е длъжно да уведоми КЗЛД.
Ако Дружеството, към момента на подаване на уведомлението до КЗЛД, все още не е съобщило на субекта на данните за нарушението на сигурността на неговите лични данни, КЗЛД може, след като отчете каква е вероятността нарушението на сигурността на личните данни да породи висок риск, да изиска от Дружеството да съобщи за нарушението. В този случай, Дружеството, следвайки указанията на КЗЛД, следва да предприеме действия по уведомяването на субектите на данни по подходящ според конкретния случай начин.

Различните видове нарушения може да изискват допълнителна информация, която да бъде предоставена, за да се обяснят напълно обстоятелствата по всеки конкретен казус.

Липсата на точна информация (например точен брой засегнати лица), не е пречка за своевременното уведомяване на КЗЛД. В такива случаи следва да бъдат описани приблизителния брой на засегнатите лица.

Ако не е възможно необходимата информацията да се подаде едновременно с уведомлението до КЗЛД, същата може да се подаде поетапно без ненужно забавяне. Предпоставки за такова поетапно уведомяване са:

- Не са налице всички релевантни факти;
- Нарушението на сигурността е с по-голяма фактическа сложност (например някои видове

инциденти в областта на киберсигурността);
- Да се посочат причините за забавянето и КЗЛД да бъде уведомена своевременно, че е налице невъзможност да бъде предоставена пълната информация;
- Да бъде получено одобрението на КЗЛД за такова поетапно уведомяване;
- Да бъдат получени насоки от КЗЛД относно уведомяването на засегнатите субекти, дали, кога или как да бъдат уведомени

По изключение и при специфични обстоятелства е възможно отложено уведомяване – например, ако в хода на разследването се установява наличие на многократни и сходни Нарушения на сигурността за определени категории данни за кратък период от време засягащи голям брой Субекти, Дружеството може да уведоми КЛЗД за всички тях едновременно, надхвърляйки срока от 72 часа. Тази възможност следва да се прилага ограничително и при стриктно отчитане спецификите на конкретния случай.

Уведомлението до надзорния орган в тези случаи следва да съдържа причините за забавянето.

ОЦЕНКА НА РИСКА

Веднага щом получи сигнал за евентуално Нарушение на сигурността или има съмнения за такова, Екипът за реакция пристъпва към следния план за действие (при предоставяне от Дружеството на необходимите ресурси/ допълнителни експертни знания, ако се налага):

- оценка на риска по скала от 1 до 5 (от пренебрежим до висок; както по вероятност за настъпване, така и по интензитет) за правата на субектите с оглед на мащаба на засягане;
- определяне категориите засегнати Лични данни;
- установяване липсата/ наличието на криптиране/ други относими обстоятелства, които да минимизират риска от Нарушението на сигурността и съответно да премахнат необходимостта от уведомяване на Субектите;
- даване препоръка, въз основа степента на установения риск, относно това дали да бъде уведомена КЗЛД;
- предлагане на конкретни последващи мерки, които да ограничат риска от настъпилото Нарушение на сигурността.

Висок риск за целите на оценката съществува, когато Нарушението на сигурността има вероятност да доведе до физическа, материална или нематериална вреда за субектите, сигурността на чиито данни е нарушена. Примери за такава вреда са дискриминация, кражба на самоличност, измама, финансова загуба или накърняване репутацията. Когато Нарушението на сигурността включва Лични данни, свързани с раса или етнос, здравословно състояние, сексуална ориентация, присъди или наказателно преследване, наложени принудителни мерки в тази връзка, настъпването на физическа, материална или нематериална вреда се предполага.

При оценката на риска от Нарушението на сигурността, следва да се вземат предвид специфичните обстоятелства, включително сложността на потенциалното въздействие и вероятността от настъпване, като:

- Вида Нарушение на сигурността;

- Характерът, чувствителността и обемът на засегнатите Личните данни - колкото по-чувствителни са данните, толкова по-голям е рискът от увреждане на Субектите.

  Чувствителни могат да бъдат личните 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.

Отделно, малка част от чувствителните лични данни могат да окажат голямо влияние върху даден Субект, а широк спектър от детайли относно тези данни може да разкрие повече информация за него. Нарушение, засягащо голямо количество Лични данни за широк кръг от Субекти, също може да има съществен негативен ефект;

- Неправомерната идентификация на засегнатите Субекти от трети лица - когато е осъществен неоторизиран достъп до засегнатите Лични данни от трето лице, трябва да се вземе предвид колко лесно това лице може да идентифицира Субектите. В зависимост от обстоятелствата, идентифицирането би могло да бъде направено чрез използването на данните без допълнителни изследвания за откриване самоличността на индивида, а може и да е изключително трудно да се свържат засегнатите Лични данни с конкретен Субект, но въпреки това идентифицирането да е възможно при определени условия;

- Сериозността на настъпилите последствия за Субектите;
- Специфичните особености на Субектите;
- Специфичните характеристики на дейността на Дружеството като Администратор;
- Броят на засегнатите Субекти.

РЕГИСТЪР НА НА НАРУШЕНИЯТА

Независимо дали Нарушението на сигурността налага или не уведомяване, Дружеството документира всички факти, свързани с него, последиците му, предприетите действия, аргументите за взетите решения. Дружеството създава специален регистър за целта.
В Регистъра задължително се вписват предполагаемото време или период на възникване, времето на установяване, времето на докладване и името на служителя, извършил доклада. След анализа от Екипа за реакция, в регистъра се записват последствията от инцидента и мерките, които са предприети за отстраняването им.

ПРЕВАНТИВНИ ПРОЦЕДУРИ И МЕХАНИЗМИ

В дружеството се изготвя план за обучение на новопостъпили и/или преназначени служители, както и периодични обучения и разяснения на всички служители. При осъществяване на своята дейност, служителите се ръководят и от вътрешните политики, правила и процедури на Дружеството при обработка на лични данни.

При напускане на служители се предприемат всички необходими технически и организационни мерки, свързани със защитата на всеки регистър/категория лични данни, воден от **„АЛУМИНА ЕЛИТ 2003" ЕООД**, като например:

1) Промяна на пароли;
2) Ограничаване на достъп (вкл. ВПН, облачни услуги, сървъри и др.);
3) Връщане на всички служебни устройства, като напр. телефон, лаптоп, USB флаш памет и др. в зависимост от конкретния случай; връщането на устройства задължително се последва от изтриване на персонализиращата информация на последния ползвал служител в устройството, вкл. в случаите, когато върнатото устройство подлежи на директно бракуване/унищожаване.
4) Ограничаване на физически достъп чрез връщане на ключове, промени на кодове за достъп и др.

Криптиране на данните - в случай, че съществува повишен риск от нерегламентиран физически достъп до носители на чувствителни данни или в случай на кражба на служебни устройства, които са носители на лични данни.
В случаите на необходимост от възстановяване на данни, процедурата се изпълнява след писменото разрешение на съответното лице, отговорно за информационна сигурност, като това се отразява в регистъра по архивиране и възстановяване на данни.

В случаите на компрометирането на парола тя незабавно се подменя с нова, като сертификата за достъп на съответния служител се обезсилва, а събитието се отразява в регистъра за инциденти.

Екипът за реакция, заедно с управителя на дружеството, могат да предприемат и други превантивни мерки, механизми и вътрешни инструкции.

Настоящата Политиката е утвърдена със Заповед № 30 от 21.05.2018 г. На Управителя и е в сила от 25.05.2018 г.