Политика за защита на личните данни

C6.PLC.01

Редакция 1.0

Дата на влизане в сила: 25.04.18

Правни бележки

Търговски марки и Марки за услуги

Еврохим, логото на Еврохим и други думи или символи, използвани за идентифициране на описаните тук продукти и услуги, са или търговски марки, или търговски наименования или марки за услуги на Еврохим и неговите лицензодатели, или са собственост на съответните им собственици. Не се разрешава копирането, имитирането или използването на тези марки, изцяло или частично, без изричното предварително писмено разрешение на Еврохим. В допълнение, корици, колонтитули, персонализирани графики, икони и други елементи за дизайн е възможно да са марки за услуги, търговски марки и/или търговско оформление на Еврохим, като не е разрешено тяхното копиране, имитиране, или използване, изцяло или частично, без изричното предварително писмено разрешение на Еврохим.

Пълен списък на марките на Еврохим може да се види на страницата: http://www.eurochemgroup.com

Резюме

ИМЕ	Политика за защита на личните данни
ИДЕНТ. №	C6.PLC.01
НАДЗОРЕН ОРГАН ПО ПРОЦЕДУРАТА	А.А. Илиин, Финансов директор, Група Еврохим
СОБСТВЕНИК НА ПРОЦЕДУРАТА	В.В. Сиднев, Главен съветник, Група Еврохим
РАЗРАБОТЕНО ОТ	Е.В. Холманских, Директор „Нормативно съответствие“, Група Еврохим
РЕДАКЦИЯ	1.0
ДАТА НА ВЛИЗАНЕ В СИЛА	25.04.18
ДАТА НА ОДОБРЕНИЕ	24.04.18

Редакции

Редакция	Дата на влизане в сила	Цел	Данни за редакцията
1.0	25.04.18		Няма.

Съдържание

1. Термини и определения

Освен ако е посочено твърдение в обратния смисъл, думи и изрази, които са дефинирани (или е посочено, че са предмет на конкретно тълкуване) в Кодекса за поведение и Политиката за съответствие, имат същото значение (или подлежат на същото тълкуване) и в настоящата Политика за защита на личните данни ("Политиката").

Освен това, ще се прилагат следните определения:

Термин	Определение
"Лични данни"	означава всяка информация, свързана с идентифициран или идентифицируем Субект на данни; това е много широка гама от лични идентификатори, включително име на физическото лице, (служебен) телефонен номер, (служебен) имейл адрес, идентификационен номер, данни за местоположението, онлайн идентификатор и др.
"Чувствителни данни"	означава Лични 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 уникално идентифициране на физическото лице, данни за здравето или данни относно сексуалния живот или сексуална ориентация на физическото лице.
"Администратор на данни" или " Администратор"	означава физическо или юридическо лице, обществен орган, агенция или друг орган, който самостоятелно или съвместно с други определя целите и средствата за обработването на лични данни.
"Обработващ данни" или "Обработващ"	означава физическо или юридическо лице, което обработва личните данни от името на Администратора.
"Субект на данни"	означава всяко съществуващо лице, което е субект на Лични данни, съхранявани от Групата.
"Обработване"	означава всяка операция или съвкупност от операции, извършвана с Лични данни или набор от лични данни чрез автоматични или други средства, като например 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.
"Нарушение във връзка с Лични данни"	означава нарушение на сигурността, водещо до случайно или незаконосъобразно унищожаване, загуба, промяна, неразрешено разкриване или достъп до Лични данни, предавани, съхранявани или обработвани по друг начин.
"Съгласие на Субекта на данни"	означава всяко свободно дадено, конкретно, информирано и недвусмислено посочване на желанията на Субект на данни, с което той или тя, чрез изявление или ясно потвърждаващо действие, изказва съгласие за обработването на лични данни.

“Длъжностно лице по защита на данните за ЕС”	означава служител на Групата, който отговаря за разпространението на Политиката в рамките на частта от Групата, разположена в ЕС
“Длъжностно лице по защита на данните за целия свят”	означава служител на Групата, който отговаря за разпространението на Политиката в рамките на Групата
“Длъжностно лице по защита на данните за съответната държава”	означава отговорен служител на Групата
“Договор с обработващите данните”	означава договор, сключен между Групата и неин партньор относно разпространение на Политиката в рамките на съответната Група.
“График за съхранение”	означава специален график, в съответствие с който документите се съхраняват в рамките на определен срок.

2. Приложение

2.1. Предназначено използване

В настоящата Политика са представени основните принципи на Защита на личните данни и и Обработване на Лични данни, приложими за Групата.

Като работодател, клиент и доставчик, всеки член на Групата събира и използва лични данни, отнасящи се за служители, бизнес партньори, клиенти, потенциални клиенти и т.н. Докато обработката на тези лични данни е задължителна за нашите операции, Групата съзнава, че в основата на доверието във всички отношения е защитата на личните права и неприкосновеността на личния живот на всяко физическо лице. Ето защо Групата желае да спази всички изисквания относно защитата и правилното Обработване на Личните данни.

За Групата е от решаващо значение да спази изискванията за Защита на личните данни в държавите, където се извършва дейността и където постоянно пребивават Субектите на данните. Всички членове на Групата трябва да спазват местните разпоредби в целия свят, съгласно които се управляват и обработват лични данни.

Основен приоритет на Групата е да се осигурят универсално приложими, световни стандарти за боравене с личните данни. Настоящата Политика за защита на данните е общата рамка, която се прилага в Групата. Предвид разликите в местните регламенти и разнообразието от дейности, все пак е неизбежно прилагането на тези принципи за Защита на данните евентуално малко да се различава за някои членове на Групата.

Настоящата Политика се довежда до знанието на всички служители, които следва да я спазват и да изпълняват посочените в нея изисквания. Освен това, Политиката се прилага за партньори, които работят с членове на Групата и които имат или е възможно да получат достъп до Лични данни. От тези партньори ще се очаква да са прочели, да разбират и да спазват настоящата Политика.

2.2. Област на приложение и задължителни правни изисквания

Държавите, където Групата извършва дейност, могат да бъдат разделени на 3 големи групи в зависимост от местоположението: ЕС, Русия и други държави.

С изключение на централните управления в Швейцария и Русия, някои от членовете на Групата се намират в ЕС. Правилата за защита на данните в ЕС (Регламент (ЕС) 2016/679 (Общия регламент за защита на данните или "ОРЗД") са строги и се прилагат на хармонизирана основа в целия ЕС. Обхватът на приложение на ОРЗД надхвърля рамките на ЕС, тъй като регламентът се прилага и за членове на Групата, установени извън ЕС, ако Субектът на данни пребивава постоянно в ЕС.

Групата е поела ангажимент да използва принципите и задълженията съгласно ОРЗД като основа за своята Политика за защита на данните. Отделни членове на Групата, обаче, също е необходимо да спазват местните разпоредби. Настоящата Политика за защита на данните само допълва местните регламенти за Защита на данните. Съответният местен регламент се ползва с приоритет, ако е в противоречие с настоящата Политика за защита на данните,

или има по-строги изисквания от нея. Примери за местни разпоредби, които се отнасят за някои от членовете на Групата, включват:

- Федерален закон № 152-FZ относно личните данни от 2006 г. (приложим за Русия);
- Федерален закон относно защита на данните (ФЗЗД) от 19 юни 1992 г. (приложим за Швейцария);
- Местното законодателство по корпоративно управление и срокове на съхранение на данните.

3. Общи разпоредби

3.1. Цели на Политиката

Основните цели на Политиката са както следва:

- Да защитава правата и свободите на всички Субекти на данни и да ги информира за тях;
- Личните данни да се обработват по правилен начин;
- Да се избегнат нарушения във връзка с Лични данни и въпроси, свързани със сигурността като цяло.
- Да се повиши информираността относно режима по Защита на личните данни като цяло.

3.2. Принципи на Политиката

Всяко обработване на Лични данни трябва се извършва съобразно изложените в ОРЗД принципи за Защита на данните. Политиките и процедурите на Групата са предназначени да осигурят съответствие с тези принципи.

Накратко, ние, като Група, се ангажираме да спазваме следните принципи:

- Принципа на добросъвестност и законосъобразност: ние се ангажираме да обработваме лични данни само дотолкова, доколкото сме информирали Субекта на данни и доколкото е налице правно основание за обработването.

- Принципа на ограничаване на целите: ние ще обработваме личните данни само за конкретни, изрично указани и законни цели и няма да обработваме допълнително тези данни по начин, който е несъвместим с тези цели.

- Принципа за свеждане на данните до минимум: ние ще обработваме само личните данни, които са адекватни, релевантни и ограничени до необходимото, предвид целите, за които се обработват.

- Принципа за точност: ние ще обработваме само данни, които са точни и, ако е необходимо, актуализирани. Ние ще предприемем всички разумни стъпки, за да осигурим незабавното коригиране или заличаване на лични данни, които са неточни.

- Принципа на ограничаване на обработването: ние ще съхраняваме всички лични данни във форма, позволяваща идентифицирането на Субектите на данните, не по-дълго, отколкото е необходимо за целите, за които се обработват.

- Принципа за сигурността: ние ще обработваме данни само по начин, който осигурява подходяща сигурност, включително защита срещу неразрешено или неправомерно обработване и срещу случайна загуба, унищожаване или увреждане, като използваме всички подходящи технически или организационни мерки.

- Принципа за отчетност: ние ще носим отговорност за, и във всеки момент ще можем да докажем съответствие с горепосочените принципи за Защита на данните както пред компетентните органи, така и пред Субектите на данните.

4. Мерки за защита на данните

Свидетелство за ангажимента на Групата да прилага гореспоменатите принципи за Защита на данните са следните мерки, които сме предприели:

4.1. Законосъобразно и добросъвестно обработване

Групата осигурява добросъвестното и законосъобразно събиране и обработване на данните. Ние предприемаме всички разумни стъпки, за да осигурим актуалност и точност на личните данни и съхраняването им само за предварително определения срок.

Групата осигурява използването на събраните данни, в зависимост от категорията, към която принадлежи Субектът на данни, само в съответствие с описаните по-долу добросъвестни и законосъобразни основания.

4.1.1. Данни на служителите

„Данни на служителите“ означава всички данни, обработвани от всеки член на Групата, които са свързани със служителите и (при необходимост) техните брачни партньори. „Данни на служителите“, обаче, има по-широк смисъл от лични данни на настоящите служители. Съществуват и други категории данни, свързани с трудовото правоотношение, като например данни за пенсионирани служители и кандидати за работа.

Всички данни на служителите се събират от Групата, в която е назначен служителят. Работодателят се счита за Администратор на данните (което означава, че Групата определя целите и средствата за обработването на данните).

1. законно основание за дейностите по обработване

В трудовото правоотношение по-голямата част от дейностите по обработване на данни се легитимира от необходимостта от изпълнение на определен договор: членове на Групата няма да могат надлежно да изпълняват задълженията си по своите трудови договори без да могат да обработват данни на своите служители.

Някои от дейностите по обработване на данни се легитимират от правно задължение: във всички държави, където членовете на Групата извършват дейност, е налице правно

задължение да се обработват някои лични данни на служителите, например поради причини, свързани със социалното осигуряване, застраховки, изплащане на заплати и т.н.

Някои от дейностите по обработване на данни могат да бъдат разрешени и съгласно колективните договори. Колективните договори са договори съгласно утвърдени ставки или договори между работодатели и представители на служителите, в рамките на обхвата, разрешен съгласно съответния закон за трудовите правоотношения. Договорите трябва да покриват конкретните цели на предвидената дейност по обработване, като трябва да бъдат изготвени в рамките на параметрите на националното законодателство за Защита на данните.

Всеки член на Групата в почти всички случаи може да се позове и на законни интереси за обработване на лични данни, тъй като това е необходимо за правилното функциониране на неговата дейност (например въпреки че определен член на Групата няма трудов договор с кандидати, Групата има законен интерес да оцени потенциалните кандидати, особено когато те инициират процедурата за кандидатстване чрез свързване с члена на Групата).

В много ограничен брой случаи е възможно да се наложи дейностите по обработване да се легитимират с изрично съгласие, дадено от служителя (например: публикуване на интервю или снимка във вътрешен бюлетин и т.н.).

Всеки член на Групата носи самостоятелна отговорност за посочване на законното основание за дейностите по обработване.

2. добросъвестно обработване

Подробен преглед на това как се обработват данните на служителите е представен в нашите по-подробни политики. Тук представяме кратък преглед на някои аспекти на дейността по обработване:

- Свеждане до минимум: Групата осигурява ограничаване до минимум на обработването на данните на служителите.
- Точност: Групата осигурява редовното актуализиране на всички данни на служителите на ниво юридическо лице, като всеки служител може по всяко време да поиска да бъдат коригирани грешни данни.
- Ограничаване срока на съхранение: всички данни на служителите ще бъдат обработвани за срока на техния трудов договор. След прекратяване на трудовия договор голяма част от данните ще бъдат изтрити, след като е спазен необходимият срок за запазване, освен ако в закона е предвидено друго, или Субектът на данни изрично се е съгласил данните му да останат за по-нататъшни конкретни дейности по обработване.
- Сигурност: Всички лични данни се обработват по защитен начин. Например: достъпът до данните е ограничен на база осведомяване само в случай на необходимост, Групата често псевдонимизира данни, когато се прехвърлят към трето лице и т.н.
- Обработване на чувствителни данни: чувствителни данни, като например данни за расов и етнически произход, политически убеждения, религиозни или философски убеждения, членство в професионални съюзи и данни за здравето и сексуалния живот на Субекта на данни ще бъдат обработвани с необходимата допълнителна грижа.
- Групата свежда до минимум автоматичното обработване на лични данни. Ако личните данни се обработват автоматично в рамките на трудовото правоотношение

и се оценяват конкретни лични данни (например в рамките на подбор на персонал или за оценка на профили в съответствие с уменията), това автоматично обработване не може да бъде единственото основание за решения, които биха имали отрицателни последици или биха причинили значителни проблеми за засегнатия служител.

Всеки член на Групата носи самостоятелна отговорност за добросъвестното обработване на данните на служителите.

4.1.2. Данни на партньорите

„Данни на партньорите“ означава лични данни на клиенти, подизпълнители, доставчици, бизнес партньори, посетители на уебсайта и др. Въпреки че това винаги ще бъдат професионални данни, което означава, че няма да бъдат обработвани почти никакви чувствителни данни, всеки имейл адрес или телефонен номер ще се счита за лични данни.

Доколкото Групата е събрала данните на партньорите директно от съответния Субект на данни, тя ще функционира като Администратор на данни. Естеството на дейността на Групата може да наложи данните на партньорите да се събират от някоя друга страна. В този случай Групата ще бъде само Обработващ данни, а не Администратор на данни, освен ако е договорено друго.

1. законосъобразно основание за дейностите по обработване

В договорното отношение по-голямата част от дейностите по обработване на данни се легитимира от необходимостта, породена от изпълнение на договор: Групата няма да може да изпълнява надлежно задълженията си по своите договори, без да може да обработва съответните данни.

Някои от дейностите по обработване на данни се легитимират от правно задължение: в някои държави, където оперира Групата, е налице правно задължение да се обработват определени лични данни от страна на доставчиците.

В почти всички случаи Групата може да се позове на законни интереси да обработва лични данни, тъй като това е необходимо за правилното функциониране на нейната дейност.

В много ограничен брой случаи е възможно дейностите по обработване да е необходимо да се легитимират с изрично съгласие, дадено от трето лице (например: получаване на бюлетин на Групата, и т.н.).

Доколкото Данните на партньорите се контролират от Групата (което означава, че целите и средствата за обработването на данни се определят от член на Групата), тази Група ще бъде отговорна за посочване на законосъобразното основание за дейностите по обработване.

2. добросъвестно обработване

Подробен преглед на това как се обработват данните на партньорите, може да се открие в нашите по-подробни политики. Като цяло, се прилагат същите принципи като прилаганите за обработването на данните на служителите, както е описано в точка 4.1.1.

Следва да се обърне внимание на следните допълнителни принципи:

- В случай че обработването на данните на партньорите се събират чрез уебсайта на Групата и онлайн инструменти: ако се събират, обработват и използват лични данни

в уебсайтове, Субектите на данните ще бъдат информирани за това в уведомление за неприкосновеност и, ако е приложимо, информация относно бисквитките. Уведомлението за неприкосновеност и всяка информация относно бисквитка ще бъдат интегрирани така, че лесно да се идентифицират и да са директно достъпни и постоянно на разположение на Субектите на данните.

Доколкото създаваме потребителски профили (проследяване) на нашите сайтове, Субектите на данните винаги ще бъдат съответно уведомени за това в уведомлението за неприкосновеност. Лично проследяване може да се осъществи само ако е разрешено съгласно националното законодателство или при съгласие на Субекта на данни.

В случай че уебсайтове или приложения могат да осъществяват достъп до лични данни в зона, достъпна само за регистрирани потребители, идентификацията и удостоверяването на Субект на данни ще предлагат достатъчна защита по време на осъществяване на достъп.

- Дигитален маркетинг: Групата осъществява стратегии за дигитален маркетинг главно в контекст "бизнес към бизнес", където няма законово изискване да се получава съгласие за извършване на дигитален маркетинг към физически лица, при условие, че те получават възможност да се откажат.

  Като общо правило, обаче, Групата ще се стреми винаги да получава съгласие преди изпращане на рекламни материали или материали за директен маркетинг на партньор, който е Субект на данни.

Доколкото Групата е Администраторът на данните на партньорите, Групата ще отговаря за идентифициране на законосъобразното основание за дейностите по обработване.

4.1.3. Съгласие

Доколкото Групата се позовава на съгласието като законосъобразно основание за обработване, ще се прилагат следните условия:

Декларациите за съгласие ще бъдат предоставяни доброволно, в писмена форма и в съответствие с местните разпоредби. Всяко съгласие, което не отговаря на тези условия, е нищожно. Декларацията за съгласие ще се получава в писмена форма или по електронен път с цел документиране. Преди да даде съгласие, Субектът на данни ще бъде информиран за степента, до която ще се извършват дейности по обработване. Субектът на данни може да оттегли съгласието си по всяко време.

За Чувствителни данни трябва да бъде получено изрично писмено съгласие на Субектите на данните, освен ако съществува ясно алтернативно легитимно основание за обработване.

В повечето случаи Групата обичайно получава съгласието за обработване на Лични и Чувствителни данни, като използва стандартни документи за съгласие.

4.2. Защита правата на Субектите на данните

Всеки член на Групата осигурява възможност Субектът на данни, чиито Лични данни се обработват от Групата, да може да упражнява следните индивидуални права.

- **Правото да бъде информиран:**

Политиката осигурява пълен преглед на общите принципи, при които Групата обработва Лични данни. Тя е споделена със Субектите на данните в момента на събиране на Лични данни (доколкото Групата е Администраторът) и е публично достъпна на www.eurochemgroup.ru.

В случай че Субект на данни изрично поиска това, обаче, съответният член на Групата (което означава Администраторът или Обработващият Лични данни) ще предостави на Субекта на данни информацията за неговите Лични данни в спретната, прозрачна, разбираема и лесно достъпна форма. Групата си запазва правото да откаже искане за информация, доколкото Субект на данни вече разполага с информацията, или ако това би било свързано с прекомерно усилие за предоставянето ѝ.

При поискване, Групата предоставя следната информация: 1) името и данните за контакт на юридическото лице, 2) целите на обработването, 3) законосъобразното основание за обработването; 4) категориите получени Лични данни; 5) получателите или категориите получатели на личните данни, 6) данните за трансферите на Лични данни към трети държави или международни организации (ако е приложимо), 7) сроковете за съхранение за личните данни, 8) правата, предоставени на Субектите на данните по отношение на обработването, 9) правото съгласието да се оттегли (ако е приложимо), 10) правото да се подаде оплакване до надзорен орган.

- **Правото на достъп:**

  За да се осигури възможност Субектите на данните да са информирани и да могат да проверят законосъобразността на дейностите по обработване, Групата им предоставя право да получат потвърждение, че се обработват данни на Субекта на данни; достъп до личните данни; и друга необходима допълнителна информация. Форматът на достъп е взаимно съгласуван.

- **Право на коригиране:**

  В случай че член на Групата обработва неточни или непълни лични данни, Субектът на данни може да поиска данните да се коригират или допълнят. Следователно Групата си запазва правото да откаже искане за коригиране, когато това е разрешено съгласно приложимото законодателство.

- **Право на заличаване и право на ограничаване на обработването:**

  Субектите на данните имат право техните Лични данни да бъдат заличени от записите на Групата, в случай че 1) Личните данни вече не са необходими за целите на първоначалното им събиране или обработване; 2) член на Групата се позовава единствено на съгласие като законосъобразно основание за съхранение на данните, а Субектът на данни оттегли своето съгласие; 3) член на Групата се позовава единствено на законни интереси като основание за обработване, Субектът на данни възрази срещу обработването на неговите данни и не е налице висш законен интерес

това обработване да продължи; 4) член на Групата обработва Лични данни за целите на директен маркетинг; 5) член на Групата обработва Лични данни незаконно.

Като алтернатива на искането за заличаване на лични данни, Субектът на данни може да поиска съответен член на Групата да ограничи обработването на неговите Лични данни до съхраняване на данни, но да не се използват по друг начин. Такова ограничение може да бъде поискано, ако: 1) Субектът на данни оспори точността на неговите Лични данни и член на Групата междувременно извършва проверка на точността на данните; 2) данните са били обработвани незаконосъобразно и Субектът на данни се противопостави на заличаване, като вместо това поиска ограничение; 3) Личните данни вече не са необходими на съответния член на Групата, но на Субекта на данните е необходимо те да се запазят с цел установяване, упражняване или защита на съдебен иск; 4) Субектът на данни е възразил срещу това член на Групата да обработва данните, а този член междувременно обмисля дали неговите законни се ползват с предимство пред тези на Субекта на данни.

- **Право на преносимост на данните:**

  При строго определени условия Субектът на данни може да поиска член на Групата да му предостави всички негови Лични данни в структуриран, широко използван, пригоден за машинно четене формат. Това трябва да позволява на Субекта на данни да предава своите данни към друга организация. Ако това е технически осъществимо, Субект на данни може да поиска данните да бъдат предадени директно към тази друга организация.

  Правото на преносимост на данните се прилага само: 1) за Лични данни, които съответното лице е предоставило на Администратор; 2) когато обработването се основава на съгласието на Субекта на данни или за изпълнение на договор; и 3) когато обработването се извършва чрез автоматични средства.

- **Право на възражение:**

  В случай че Субект на данни възрази срещу обработването на неговите Лични данни на "основания, свързани с конкретното му/ѝ положение", Субектът на данни има право да възрази срещу: 1) обработване на базата на законни интереси и 2) директен маркетинг (включително профилиране).

  В този случай, съответният член на Групата ще преустанови обработването на Личните данни, освен ако: 1) може да представи неоспорими легитимни основания за обработването, които се ползват с предимство пред интересите, правата и свободите на Субекта на данни; или 2) обработването е с цел установяване, упражняване или защита на правни искове.

Всички заявки за изпълнението на горепосочените права трябва да бъдат насочени към Длъжностното лице по защита на данните. Освен ако съгласно приложимото законодателство е разрешено друго, всяко искане трябва да се направи в писмена форма.

Освен ако от приложим регламент е предвидено друго, отговорът на всяка заявка ще бъде предоставен в рамките на 30 дни от получаване на писменото искане от Субекта на данни. Подходяща проверка трябва да потвърди, че заявителят е именно Субектът на данни или негов законен представител.

Освен ако от приложим регламент е предвидено друго, всяка заявка ще бъде безплатна, освен ако искането бъде счетено за ненужно или прекомерно по своето естество.

4.3. Сигурност на Личните данни

Групата се ангажира да спазва считаното за най-добра практика в отрасъла във връзка с ИТ-сигурност.

Освен това всяко Дружество от Групата е приела физически, технически и организационни мерки за осигуряване на сигурността на личните данни. Това включва предотвратяване на загуба или повреда, неразрешено изменение, достъп или обработване, както и други рискове, на които може да бъде изложен поради човешко действие или физическа или естествена среда.

Макар че мерките за сигурност са различни и зависят от члена на Групата, следните мерки ще се считат за минимални предпазни мерки:

Всички Лични данни се разглеждат като подлежащи на най-висока степен на сигурност и трябва да се съхраняват:

- в стая с възможност за заключване с контролиран достъп; и/или
- в заключен шкаф с чекмеджета или картотека; и/или
- ако са компютъризирани – да са защитени с парола в съответствие с корпоративните изисквания; и/или
- на (сменяеми) компютърни медии, които могат да се кодират.

Ръчни записи не е разрешено да бъдат оставяни на места, където до тях може да бъде осъществен достъп от неоторизирани лица и не е разрешено да бъдат премахвани от бизнес помещенията без специално разрешение. След като ръчните записи вече не са необходими за текущата работа с клиенти, те трябва да бъдат премахнати от защитеното архивиране.

Лични данни могат да бъдат изтривани или унищожавани само в съответствие с Графика за съхранение.

Групата трябва да не допуска разкриването на Лични данни пред неоторизирани партньори, включително членове на семейството, приятели, държавни органи, освен ако това се изисква от закона. Всички искания за предоставяне на данни поради някоя от тези причини трябва да бъдат удостоверявани със съответните документи и всички такива разкривания трябва да бъде изрично разрешени от Длъжностното лице по защита на данните.

Всеки член на Групата осигурява спазването от всички служители на настоящата Политика и Кодексите за поведение. Освен това всеки член на Групата гарантира, че всички служители, отговарящи за изпълнението на Политиката, ще получат съответното обучение, ще бъдат информирани и ще им бъде осигурено съответното съдействие (вж. също член 4.6)

4.4. Нарушения във връзка с Лични данни

„Нарушение във връзка с Лични данни“ е нарушение на сигурността, водещо до случайно или незаконосъобразно унищожаване, загуба, промяна, неразрешено разкриване или достъп до Лични данни, предавани, съхранявани или обработвани по друг начин. То може да възникне чрез технически или физически инцидент. Като се има предвид, че такива нарушения винаги са напълно изненадващи, всеки член на Групата е предприел всички разумни подготвителни мерки, за да се предотврати опасността някое нарушение свързано с лични данни да завърши със сериозни последици.

Всеки член на Групата е въвел ясни процедури за разкриване, разследване и докладване на нарушения. Те са описани в Политиката на Дружеството от Групата относно нарушения, свързани с данни. В допълнение, всеки член на Групата поддържа регистър на нарушенията, свързани с данни, в който се съдържа информация относно фактите, свързани с всички нарушения с лични данни, последиците от нарушенията и предприетите мерки и коригиращи действия.

Въпреки че е възможно политиките на различните членове да се различават една от друга, всяка процедура във връзка с нарушение, свързано с данни, ще съдържа следните стъпки:

- Всички служители трябва незабавно да уведомят своя пряк ръководител за случаите на нарушения на настоящата Политика за защита на данните или други разпоредби за защита на личните данни (Инциденти, свързани със защита на данните). Прекият ръководител впоследствие уведомява Длъжностното лице по защита на данните за съответната държава, Длъжностното лице по защита на данните за ЕС и Длъжностното лице по защита на данните за целия свят.

- Длъжностните лица по защита на данните решават дали Инцидентът, свързан със защита на данните, действително е довел до нарушение, свързано с лични данни. Например, изгубени USB-устройства, откраднати лаптопи, заразяване със зловреден софтуер или проникнати от хакери бази данни, съдържащи лични данни, се считат за нарушения, свързани с лични данни. Заплаха или пропуски в мерките за сигурност, като например слаби пароли или остарели защитни стени, не се считат за нарушение, свързано с лични данни, стига да не е допуснато изтичане на лични данни.

- В случай че Инцидентът, свързан със защита на данните, действително е нарушение на личните данни, Длъжностните лица по защита на данните ще разследват обхвата на нарушението. Те ще проучат обхвата на нарушението, свързано с лични данни, колко субекти на данни е възможно да бъдат засегнати, дали нарушението може да доведе до риск за правата и свободите на Субектите на данните, дали компрометираните лични данни съдържат Чувствителни данни, дали компрометираните данни са били защитени (чрез кодиране или по друг начин), дали други страни евентуално участват в нарушението, свързано с данни и какви стъпки трябва да бъдат предприети за намаляване на (по-нататъшна) загуба на Лични данни.

- Въз основа на горната оценка, Длъжностните лица по защита на данните ще решат дали съответният надзорен орган и Субектът на данни трябва да бъдат информирани за нарушението. Уведомяване на надзорния орган не е необходимо, ако е малко

вероятно нарушението във връзка с Лични данни да доведе до риск за правата и свободите на физически лица.

- В случай че е необходимо уведомяване за нарушението, свързано с лични данни, Групата ще уведоми компетентния надзорен орган и ще му представи цялата необходима информация в рамките на 72 часа, след като е узнала за нарушението.

- Когато нарушение, свързано с лични данни, е вероятно да доведе до "висока степен на риск" за правата и свободите на определени лица, Групата ще уведоми заинтересованите лица директно. 'Висока степен на риск" означава, че прагът за уведомяване на лицата е по-висок, отколкото за уведомяване на съответния надзорен орган. Ако отделните уведомления биха представлявали прекомерно усилие, Групата може вместо това да използва форма на публично съобщение, при условие, че то ще бъде също толкова ефективно за информирането на физическите лица.

- С цел поддържане на високо ниво на видимост и прозрачност, всеки член на Групата ще документира всички Инциденти, свързани със защита на данните (независимо дали са докладвани или не), включително фактите, свързани с нарушението, неговите последици и предприетите или планирани действия. Цялата тази документация трябва да може да осигури възможност на Надзорния орган да се провери спазването на задълженията за уведомяване. Всички факти за нарушението, свързано с данни, трябва да се събират в специален образец “Регистър на нарушения, свързани с данни” (Анекс 2).

4.5. Запазване и унищожаване на данни

Както вече бе посочено съгласно член 4.1 от настоящата Политика, Лични данни не могат да се обработват за срок, по-дълъг от необходимия за целите на тяхното обработване.

Всеки член на Групата е определил и създал отделен График за съхранение в съответствие с Анекс 3. Сроковете на съхранение се основават на изискванията в местното законодателство относно различните видове категории Лични данни. Обикновено местното законодателство категоризира личните данни, както следва:

1. Счетоводство и финанси
2. Договори
3. Корпоративни записи
4. Кореспонденция и вътрешни меморандуми
5. Имейли и други електронни съобщения
6. Юридически файлове и документи
7. Документи, свързани с работната заплата
8. Документи относно пенсия
9. Записи, свързани с персонала
10. Данъчни записи

Във всеки случай, всички лични данни ще бъдат запазени за минимален период, който да позволява на Групата да подаде иск или да се защити в съда в съответствие с местното законодателство.

4.6. Обучение на персонала

Групата осигурява запознаването на всички служители, които имат достъп до Лични данни, със задълженията им по настоящата Политика в рамките на тяхното обучение във връзка с въвеждането им в началото на трудовото правоотношение. В допълнение, всеки член на Групата ще осигурява редовно обучение по Защита на данните и процедурни насоки за своите служители.

Длъжностното лице по защита на данните за съответната държава носи отговорност за осигуряването на подходящи обучения за всички Служители. Форматът на такива обучения може да варира в зависимост от съответната аудитория, броя служители, които трябва да бъдат обучени, целите на обучението и други обстоятелства.

Обученията се извършват редовно. Всеки член на Групата самостоятелно определя конкретен график дати, като той трябва да е в съответствие с изискванията/ предложенията на Длъжностното лице по защита на данните за целия свят или за ЕС.

4.7. Записи на дейностите по обработване

Всяко Дружество от Групата е очертало всички Лични данни, които обработва и върху които има контрол, като ги регистрира в Регистър на данни (Анекс 4).

Чрез този Регистър на данни се осигурява спазването от страна на Дружествата от Групата определени основни изисквания за отчетност, изисквана съгласно ОРЗД:

- Водене на записи за всички дейности по обработване;
- Водене на записи във връзка с договорите с обработващите данните;
- Водене на записи на нарушенията, свързани с данни, включително уведомленията за нарушения до контролните органи и Субектите на данните.

Въпреки че съдържанието на Регистъра на данни може да варира при различните членове на Групата, той съдържа най-малко следните записи на дейностите по обработване:

- наименованието и данните за контакт на Групата и – ако е приложимо – (съвместният) Администратор и неговият представител;
- целите на дейностите по обработване;
- описание на категориите Субекти на данни и на категориите лични данни;
- категориите получатели, на които са били или ще бъдат оповестени Лични данни, включително получателите в трети държави или международни организации;
- ако е приложимо – пренос на Лични данни към трета държава или международна организация, включително посочване на тази трета държава или международна организация;

- където е възможно, предвидените срокове за заличаване на различните категории данни;

- където е възможно, общо описание на технически и организационни мерки за сигурност, взети от Групата.

Всеки от членовете на Групата носи самостоятелна отговорност за воденето на регистъра.

4.8. Пренос на данни

За да се компенсира евентуална липса на Защита на данните, преносът на Лични данни към партньори е предмет на допълнителни мерки за сигурност. Групата е определила три различни пакета трансфери на данни в рамките на своята организация – всички с различен пакет от мерки за сигурност:

- Вътрешногруповите трансфери на данни: за да се улесни преносът на данни, ще бъдат приложени Задължителни фирмени правила. Това са правила, одобрени от надзорния орган, които са правно обвързващи за всички членове на Групата. Наред с другото, тези Задължителни фирмени правила определят целите на трансфера и засегнатите категории данни; отразяват изискванията на ОРЗД; потвърждават, че износителите на база данни, намиращи се в ЕС, носят отговорност от името на цялата група; обясняват процедурите за оплаквания; и предоставят механизми за осигуряване на съответствие (например одити).

- Трансфери на данни към партньори в рамките на ЕИП (или някоя от другите държави, за които се счита, че осигуряват същата защита), действащи като Обработващ данните: това са трансфери на данни съгласно ОРЗД.

  Преди извършване на пренос на данни към трето лице, всеки член на Групата е направил запитване чрез процедури за правен анализ и е преценил дали този партньор отговаря на изискванията на приложимите регламенти.

  След тази оценка всеки член на Групата трябва да сключи договор с всяко от тези Трети лица- Обработващи данни (Договор на трето лице-Обработващо данни). Всички тези договори следва да съдържат най-малко следната информация:

- за трансферите на данни към юридически лица извън Групата извън ЕИП и доколкото се прилага ОРЗД (което означава: член на Групата се намира в рамките на ЕС или Субектът на данни пребивава постоянно в ЕС):

  В допълнение към сключване на горепосочения договор за обработване на данни, всеки член на Групата следва да провери дали партньорът, на когото ще бъдат изпратени Лични данни, поддържа подходящи допълнителни предпазни средства. Ако не са предприети такива предпазни средства, тогава Групата не прехвърля информация към това трето лице.

4.9. Оценка на въздействието върху защитата на данните

За да осигури автоматичното посочване и спазване на всички изисквания във връзка със Защита на данните при проектиране на нови системи или процеси и/или при преглед или разширяване на съществуващи системи или процеси, всеки член на Групата трябва да осигури провеждането на Оценка на въздействието върху защитата на данните (ОВЗД) за всички нови или ревизирани системи или процеси, за които носи отговорност.

Тази ОВЗД се провежда в сътрудничество с Длъжностното лице по защита на данните за целия свят и за ЕС. Където е приложимо, отделът по информационни технологии (ИТ), в рамките на своята процедура за преглед на ИТ системата и проект на приложенията, ще си сътрудничи с Длъжностното лице по защита на данните за оценка на въздействието на всяка нова технология, използвана във връзка със сигурността на личните данни.

4.10. Длъжностни лица по защита на данните

4.10.1. Длъжностните лица по защита на данните

Тъй като Групата работи в различни юрисдикции, включително ЕС, са назначени няколко Длъжностни лица по защита на данните:

- Длъжностно лице по защита на данните за целия свят (отговарящо за Групата):

  Длъжностното лице по защита на данните за целия свят се назначава и отстранява от длъжност от изпълнителния директор след консултация с Главния съветник и Финансовия директор.

  Длъжностното лице по защита на данните за целия свят на Групата е Александър Пусанов. Неговите данни за контакт са: Aleksander.Puzanov@Eurochem.ru.

- Длъжностно лице по защита на данните за ЕС (отговарящо за дейностите на Групата в рамките на ЕС):

  Длъжностното лице по защита на данните за ЕС се назначава и отстранява от длъжност от изпълнителния директор, след консултация с Длъжностното лице по защита на данните за целия свят.

  Длъжностното лице по защита на данните за ЕС на Групата е Питер Каленс. Неговите данни за контакт са: Pieter.Callens@Еврохим.be

- Длъжностни лица по защита на данните за съответната държава (отговарящи за член на Групата, ако такива бъдат назначени):

  Всеки член на Групата може да назначи Длъжностно лице по защита на данните за съответната държава. Длъжностното лице по защита на данните за съответната държава се назначава и отстранява от длъжност от изпълнителния директор/ главния управител на съответния член на Групата. В случай че не е определено Длъжностно лице по защита на данните за съответната държава, функциите на Длъжностно лице по защита на данните за съответната държава се изпълняват от изпълнителния директор/ главния управител.

4.10.2. Отговорности на Длъжностните лица по защита на данните

Длъжностно лице по защита на данните за целия свят

Длъжностното лице по защита на данните за целия свят се назначава въз основа на професионалните качества и по-специално експертни познания по законодателството и практиките във връзка със Защита на данните и способността да се изпълняват следните задължения на Длъжностното лице по защита на данните за целия свят:

- да консултира ръководството на Групата по въпроси, свързани с Политиката и да му съдейства при значителни рискове, проблеми и въпроси във връзка със Защитата на данните, в случай че възникнат такива;
- да установи и осигури висококачествена Система за защита на данните в рамките на Групата;
- да управлява стратегиите и инициативите относно комуникации, образование или обучение и да осигурява подкрепа за Бизнес звената в областта на Защита на данните според изискванията;
- да контролира Длъжностното лице по защита на данните за ЕС и Длъжностните лица по защита на данните за съответната държава (ако такива бъдат назначени) .

В сътрудничество с Длъжностното лице по защита на данните за ЕС и Длъжностните лица по защита на данните за съответната държава (ако такива бъдат назначени):

- да осигури въвеждането на подходящи процедури и политики в Групата, така че Личните данни да са точни и актуални, като се отчита обемът на събраните данни, скоростта, с която те могат да се променят и други релевантни фактори;
- да провежда редовни обучения относно Защита на данните, да предоставя обяснения за свързаните с тях въпроси и проблеми;
- да информира и консултира Групата и служителите, които извършват обработване, за техните задължения по силата на настоящата Политика;
- да наблюдава спазването на настоящата Политика и да провежда одити;
- да предоставя консултации при поискване относно Оценката на въздействието върху защитата на данните и да наблюдава нейното изпълнение;
- да наблюдава и анализира промените в приложимото законодателство;
- да извършва преглед на сроковете за съхранение на всички обработени от Групата Лични данни, като установява кои данни вече не се изискват в контекста на регистрираната цел;
- да извърши необходимото, когато на определен партньор са предадени неточни или остарели лични данни, за да го информира, че информацията е неточна или остаряла и не следва да се използва за съобщаване на решения за съответните лица; както и за предаване на всяка корекция на Лични данни към партньора, където това се изисква;
- да разгледа степента на евентуални вреди или загуби, които може да бъдат причинени на физически лица (например служители или партньор), ако възникне нарушаване на сигурността, последиците от всяко нарушение на сигурността върху самата Група и всички евентуални вреди върху репутацията, включително възможна загуба на доверието на клиента.

Длъжностно лице по защита на данните за ЕС

Длъжностното лице по защита на данните за ЕС е лице с постоянно местожителство в ЕС и се назначава въз основа на професионалните качества и по-специално експертни познания по законодателството и практиките във връзка със Защита на данните и способността да се изпълняват следните задължения в допълнение към задълженията, посочени по-горе:

- да си сътрудничи с надзорните органи на ЕС, Длъжностното лице по защита на данните за целия свят и Длъжностните лица по защита на данните за съответната държава (ако такива бъдат назначени);
- да действа като лице за контакт за надзорните органи по въпроси, свързани с обработване и нарушения, свързани с данни;
- да наблюдава и анализира промените в законодателството на ЕС и да докладва на Длъжностните лица по защита на данните за целия свят за тези промени.

Длъжностно лице по защита на данните за съответната държава

Всеки член на Групата може да назначи Длъжностното лице по защита на данните за съответната държава, което да съдейства на Длъжностните лица по защита на данните за целия свят и за ЕС при изпълнението на техните горепосочени задължения.

5. Управление на политиката

5.1. Отговорност

Всеки член на Групата носи самостоятелна отговорност за спазването на настоящата Политика, на своите правни задължения и съответното обработване на личните данни. Спазването на посочените в Политиката изисквания е задължително за служителите, участващи в процедурите.

В случай че е налице основание да се смята, че правните задължения противоречат на задълженията съгласно настоящата Политика за защита на данните, съответният член на Групата трябва да информира Длъжностното лице по защита на данните за целия свят. В случай на противоречие между националното законодателство и Политиката, Групата ще работи със съответния член на Групата с цел намиране на практично решение, което съответства на целта на Политиката за защита на данните.

Ако е подходящо, член на Групата може да приема регламенти, които допълват, или се отклоняват от настоящата Политика. Тези регламенти трябва да бъдат одобрени от Длъжностното лице по защита на данните за целия свят на Групата.

5.2. Средства за контрол

Всеки член на Групата гарантира, че спазването на изискванията в Политиката или сигнал за нарушения, които би могло да са вече извършени или потенциално да се извършат няма да доведе до отрицателни последици за съответния служител, който е техен обект. Междувременно Групата няма да приема никакви действия на служители, които нарушават Политиката.

Групата предполага и очаква, че служителите ще докладват всички случаи на нарушения или потенциални нарушения на Политиката чрез "Линията за подаване на сигнали". Данните за линията са публично достъпни и са публикувани на корпоративния портал.

Групата си запазва правото периодично да проверява доколко служителите познават Защитата на личните данни, да извършва одит на изпълнението и прилагането на настоящата Политика и да прави анализ на нейната ефективност.

5.3. Поверителност

Както е описано в член 4.4, Личните данни са предмет на задължения за поверителност.

При определени обстоятелства, обаче, е разрешено да се споделят лични данни без знанието или съгласието на съответния Субект на данни. Такъв е случаят, когато разкриването на Лични данни е необходимо за някоя от следните цели:

- Предотвратяване или разкриване на престъпления.
- Задържане или съдебно преследване на извършителите на престъпления.
- Оценка или събиране на данък или налог.
- По разпореждане на съд или съгласно правна норма.

В случай че член на Групата обработва лични данни за някоя от тези цели, тогава той може да приложи изключение от задължението си за поверителност, но само доколкото има вероятност, ако не направи това, да нанесе вреда за съответния случай.

В случай че член на Групата получи искане от съд или регулаторен или правоприлагащ орган за информация, отнасяща се за субект на данни, юридическото лице трябва незабавно да уведоми Длъжностното лице по защита на данните за целия свят, който ще осигури подробни насоки и съдействие.

5.4. Преглед на политиката

Преглед на настоящата Политика се извършва от Длъжностното лице по защита на данните за целия свят редовно, но най-малко веднъж годишно, за да се осигури актуалността и съответствието на Политиката с всички приложими правила и закони.

Всяко изменение ще бъде докладвано незабавно на Групата, която ще прилага измененията.

Последната редакция на Политиката за защита на данните може да бъде разгледана в уебсайта на Групата: www.eurochemgroup.com

5.5. Оплаквания и въпроси

Всички запитвания във връзка с настоящата Политика и нейните анекси могат да се изпращат на Длъжностното лице по защита на данните за целия свят или на съответното Длъжностно лице по защита на данните за съответната държава.

Субекти на данни, имащи оплакване във връзка с обработването на техните лични данни, трябва да представят въпроса в писмена форма на Длъжностното лице по защита на данните за целия свят. Ще бъде извършено проучване на оплакването, доколкото е целесъобразно според същността на конкретния случай. Длъжностното лице по защита на данните за целия свят ще информира субекта на данните за хода и резултата от оплакването в разумен срок.

В случай че проблемът не може да бъде решени чрез консултации между Субекта на данни и Длъжностното лице по защита на данните за целия свят, тогава Субектът на данни може по своя преценка да потърси законова защита чрез посредничество, задължителен арбитраж, по съдебен път, или чрез жалба пред съответния орган по Защита на данните в съответната юрисдикция.

.

Анекс 1. Референции

№	ID	Заглавие на документа	Remark
Регулаторен документ			
1		Политика за съответствие на „Еврохим Груп АГ“	
2		Кодекс за поведение на „Еврохим Груп АГ“	
3		Федерален закон относно защита на данните (ФЗЗД)	

Анекс 2. Регистър на нарушения, свързани с данни

№	Член на Групата	Категория лични данни	Описание	Брой засегнати Субекти на данни	Данни за контакт на Субектите на данните	Потенциални последици	Мерки, които са предприети/ следва да се предприемат

Анекс 3. График за съхранение

№	Член на Групата	Категория лични данни	Вид запис	Срок на съхранение

Анекс 4. Регистър на данни

№	Член на Групата*	Категория и описание на личните данни*	Цел на обработването*	Категории получатели*	Прехвърляне към трето лице	Срокове за заличаване	Мерки за сигурност

Колоните, отбелязани със * са задължителни полета.