26.06.2018 г.

EXIDE TECHNOLOGIES
(Exide, или «Компания»)

Политика защиты данных («Политика»)

Вы обязаны ознакомиться с данной политикой, поскольку в ней содержится важная информация о:

- принципах защиты данных, которые компания Exide обязана соблюдать;
- том, что считается персональной информацией (или данными) и конфиденциальной персональной информацией (или данными);
- каким образом Exide осуществляет сбор, использует и (в конечном счете) удаляет персональную информацию и конфиденциальную персональную информацию в соответствии с Политикой;
- том, где можно найти более подробные сведения о данных (например, о том, какую персональную информацию собирает и использует Exide, каким образом персональная информация используется, хранится и передается, для каких целей, какие меры принимаются для охраны персональной информации и как долго она хранится);
- ваших обязательствах по защите данных в качестве сотрудника Exide; и
- последствиях несоблюдения данной Политики.

1 Введение

1.1 Exide собирает, хранит и использует персональную информацию (также именуется «персональными данными») о третьих сторонах в силу нескольких законных оснований, описанных в *«уведомлениях о конфиденциальности и защите данных»* компании Exide.

1.2 В настоящей Политике описываются принципы, которыми мы руководствуемся для соблюдения наших обязательств по защите данных. Цель настоящей Политики заключается в том, чтобы довести до сведения персонала, включая сотрудников, временных работников и сотрудников, работающих через кадровое агентство, правила сбора, использования и удаления персональной информации, доступ к которой они могут получить в ходе выполнения своих рабочих обязанностей, и обеспечить соблюдение ими таких правил.

1.3 Exide стремится к соблюдению своих обязательств по защите данных и старается четко, ясно и недвусмысленно раскрывать информацию о том, каким образом Exide получает и использует информацию, и как (и когда) Exide удаляет такую информацию, когда ее дальнейшее хранение не требуется.

1.4 Если у вас есть вопросы или пожелания в отношении содержания настоящей Политики, либо вам требуется дополнительная информация, свяжитесь с местным Представителем по вопросам Общего регламента по защите данных или Юридическим отделом.

2 Область применения

2.1 Сотрудникам следует ознакомиться с уведомлениями о конфиденциальности и защите данных (при необходимости), и прочими применимыми политиками, в том числе связанными с *безопасностью информации и хранением учетных данных*, в которых содержатся сведения о защите персональной информации в соответствующем контексте.

2.2 Exide будет проводить пересмотр и актуализацию настоящей Политики в соответствии со своими обязательствами по защите данных. Настоящая Политика не является частью трудовых договоров с сотрудниками, и мы вправе вносить изменения,

актуализировать или дополнять настоящую Политику. Новая или измененная политика будет предоставлена после ее принятия.

3 Определения

информация о судимости – персональная информация, связанная с судимостями и уголовными преступлениями, обвинениями, разбирательствами и сопутствующими мерами обеспечения безопасности

нарушение безопасности данных – нарушение безопасности данных, которое приводит к случайному или незаконному уничтожению, утрате, изменению, несанкционированному раскрытию персональной информации или доступу к ней;

субъект данных – физическое лицо, к которому относится персональная информация;

персональная информация (также иногда именуется «персональными данными») – информация, относящаяся к субъекту данных, позволяющая напрямую или косвенно установить его личность с помощью такой информации;

обработка информации – получение, учет, организация, хранение, изменение, поиск, раскрытие и/или уничтожение информации либо ее использование в широком смысле или осуществление любых других действий с ней;

Псевдонимизация – процесс обработки персональной информации таким образом, который не позволяет установить личность субъекта данных без использования дополнительной, отдельно хранящейся информации, с применением технических и организационных мер, обеспечивающих невозможность определения принадлежности информации субъекту данных, личность которого может быть установлена;

конфиденциальная персональная информация (иногда именуется «особыми категориями персональных данных» или «конфиденциальными персональными данными») – следующая персональная информация о субъекте данных: раса, этническое

происхождение, политические взгляды, религиозные убеждения или философские взгляды, членство в профсоюзе (или отсутствии такового), а также генетические сведения, биометрическая информация (если используется для установления личности субъекта данных) и информация о состоянии здоровья, половой жизни или сексуальной ориентации субъекта данных.

4 Принципы защиты данных

4.1 Exide будет соблюдать следующие принципы защиты данных при обработке персональной информации:

4.1.1 мы будем осуществлять обработку персональной информации законным, добросовестным и «прозрачным» способом;

4.1.2 мы будем собирать персональную информацию исключительно в конкретных, четко сформулированных и законных целях, и не будем осуществлять обработку каким-либо образом, несовместимым с такими законными целями;

4.1.3 мы будем обрабатывать только ту персональную информацию, которая является достаточной, актуальной и необходимой для соответствующих целей;

4.1.4 мы будем хранить достоверную и актуализированную персональную информацию, а также принимать разумно обоснованные меры для удаления или исправления недостоверной персональной информации без промедления;

4.1.5 мы будем хранить персональную информацию в такой форме, которая позволяет установить личность субъекта данных, только на протяжении периода времени, когда такая информация необходима для целей ее обработки; и

4.1.6 мы будем принимать соответствующие технические и организационные меры для обеспечения безопасности и защиты информации от

несанкционированной или незаконной обработки, а также от случайной утраты, уничтожения или повреждения.

5 Основание для обработки персональной информации

5.1 До начала первичной обработки и впоследствии на регулярной основе вплоть до завершения обработки в отношении любой деятельности по обработке информации Exide будет:

5.1.1 анализировать цели конкретных мероприятий по обработке и выбирать наиболее подходящее законное основание (или основания) для такой обработки, т. е.:

(a) наличие согласия субъекта данных на обработку;

(b) наличие необходимости в обработке с целю выполнения договора, по которому субъект данных является стороной, либо с целью принятия мер по просьбе субъекта данных до заключения договора;

(c) наличие необходимости в обработке с целью соблюдения предусмотренного законодательством обязательства, применимого к Компании;

(d) наличие необходимости в обработке с целью защиты жизненно важных интересов субъекта данных или иного физического лица; или

(e) наличие необходимости в обработке для защиты законных интересов Exide, Компании или третьей стороны, за исключением случаев, когда такие интересы являются менее приоритетными в сравнении с основополагающими правами и свободами субъекта данных (см. пункт 5.2 далее).

5.1.2 анализировать необходимость в обработке для достижения цели, связанной с конкретным законным основанием (т. е. необходимость, обусловленная отсутствием других разумно обоснованных способов достижения такой цели), кроме случаев, когда обработка осуществляется на основании согласия;

5.1.3 вносить в документацию принятое нами решение касательно применимого законного основания в качестве доказательства соблюдения принципов защиты данных;

5.1.4 включать сведения как о целях обработки, так и о законном основании обработки в наши уведомления о конфиденциальности;

5.1.5 при обработке конфиденциальной персональной информации – также определять особое законное условие обработки (см. пункт 6.2.2 далее) и вносить его в документацию (только в Соединенном Королевстве); и

5.1.6 при обработке информации об уголовных преступлениях в соответствии с законодательством Европейского Союза или входящего в его состав государства – также определять законное условие обработки такой информации и вносить его в документацию.

5.2 При определении уместности законных интересов Компании в качестве подходящего основания для законной обработки мы:

5.2.1 проведем оценку законных интересов и вести учет ее результатов, чтобы обеспечить возможность обосновать наше решение;

5.2.2 если в результате оценки законных интересов будет выявлено существенное влияние на конфиденциальность, мы рассмотрим необходимость проведения оценки воздействия на защиту данных; и

5.2.3 включим информацию о наших законных интересах в соответствующие уведомления о конфиденциальности.

6 Конфиденциальная персональная информация

6.1 Конфиденциальная персональная информация иногда именуется «особыми категориями персональных данных» или «конфиденциальными персональными данными».

6.2 Компания может периодически выполнять обработку конфиденциальной персональной информации. Мы будем выполнять обработку конфиденциальной персональной информации только если:

6.2.1 у нас будет иметься законное основание согласно приведенному выше пункту 5.1.1 (например, если это необходимо для выполнения условий трудового договора, соблюдения предусмотренных законодательством обязательств Exide или в законных интересах Компании); и

6.2.2 если применяется одно из особых условий обработки конфиденциальной персональной информации, например:

(a) субъект данных в явной форме предоставил свое согласие;

(b) обработка необходима для осуществления прав по трудовому законодательству или выполнения обязательств Exide или субъекта данных;

(c) обработка необходима для защиты жизненно важных интересов субъекта данных, при этом субъект данных не имеет физической возможности предоставить согласие;

(d) обработка относится к персональным данным, которые были обнародованы субъектом данных, о чем имеются соответствующие свидетельства;

(e) обработка необходима для оформления, предъявления или осуществления защиты по судебным искам; или

(f) обработка необходима для защиты значимых общественных интересов.

6.3 Exide будет осуществлять обработку конфиденциальной персональной информации только после того, как:

6.3.1 субъекту данных будет надлежащим образом сообщено (путем направления уведомления о конфиденциальности или иным способом) о характере, целях и законном основании для обработки.

6.4 Компания обязуется не принимать автоматизированные решения (включая профилирование) на основании любой конфиденциальной персональной информации субъекта данных.

6.5 В *уведомлении о конфиденциальности и защите данных* Компании указываются типы конфиденциальной персональной информации, обработку которых выполняет Exide, цели ее использования и законное основание для обработки.

6.6 В отношении конфиденциальной персональной информации Компания обязуется соблюдать процедуры, предусмотренные приведенными далее пунктами 6.7 и 6.8 с целью обеспечения соответствия принципам защиты данных согласно пункту 4 выше.

6.7 **В период набора персонала**: Кадровый отдел Exide примет меры (если они не противоречат законодательству), чтобы:

6.7.1 при подготовке окончательного списка, проведении собеседований и принятии решений не задавались вопросы, относящиеся к конфиденциальной персональной информации (например, о расе и этническом происхождении, членстве в профсоюзе или состоянии здоровья);

6.7.2 заполненные формы, требуемые согласно принципам равных возможностей, хранились отдельно от формы заявления, поданного субъектом данных, без возможности доступа к ним лицом, подготавливающим окончательный список, проводящим собеседования или принимающим решение о трудоустройстве;

6.7.3 проверки «права на трудовую деятельность» проводились до направления кандидату окончательного предложения о работе, но не на более ранних стадиях подготовки окончательного списка, проведения собеседований и принятия решений;

6.8 **В период трудоустройства**: кадровый отдел выполнит обработку:

6.8.1 информации о состоянии здоровья в целях организации оплаты по больничным листам, учета больничных листов, контроля посещаемости сотрудников и содействия в выплатах пособий по болезни;

6.8.2 конфиденциальную персональную информацию в целях соблюдения требований к обеспечению равных возможностей. По возможности, данная информация будет анонимизирована; и

6.8.3 информации о членстве в профсоюзе в целях управления кадрами и вычета членских взносов из заработной платы.

7 Информация о судимости

Информация о судимости будет обрабатываться в соответствии с законодательством Европейского Союза или входящего в его состав государства.

8 Оценка воздействия на защиту данных (ОВЗД)

8.1 Если имеется вероятность того, что обработка приведет к риску для прав субъекта данных на защиту (например, если Exide планирует использовать новые технологии), перед началом обработки мы обязуется выполнить ОВЗД для анализа:

8.1.1 необходимости и уместности обработки с учетом цели обработки;

8.1.2 рисков для субъектов данных; и

8.1.3 мер, которые могут быть приняты для сокращения рисков и защиты персональной информации.

8.2 Перед использованием новых технологий ответственный руководитель должен связаться с Отделом информационных технологий для выполнения ОВЗД.

8.3 В ходе проведения ОВЗД Компания будет обращаться за консультациями и будет учитывать мнение всех заинтересованных сторон.

9 Документация и учет

9.1 Exide обязуется вести учет деятельности по обработке информации, включая следующее:

9.1.1 наименование и реквизиты предприятия Exide (и других контролеров, в зависимости от ситуации);

9.1.2 цель обработки;

9.1.3 описание категорий субъектов данных и категорий персональных данных;

9.1.4 категории получателей персональных данных;

9.1.5 сведения о передаче данных в другие страны, включая документацию о применяемых мерах защиты данных (если такая передача осуществляется);

9.1.6 графики хранения (при наличии возможности); и

9.1.7 описание технических и организационных мер обеспечения безопасности (при наличии возможности).

9.2 В рамках учета нашей деятельности по обработке информации мы документируем или указываем ссылку на документацию, содержащую:

9.2.1 информацию, требуемую для уведомлений о конфиденциальности;

9.2.2 данные учета предоставленных разрешений;

9.2.3 информацию о договорах между контролером и ответственным за обработку данных;

9.2.4 сведения о месте хранения персональной информации;

9.2.5 сведения о результатах ОВЗД; и

9.2.6 информацию об учете нарушений безопасности данных.

9.3 Если мы осуществляем обработку конфиденциальной персональной информации или

информации о судимости, мы будем вести учет следующего:

9.3.1 цели обработки, включая (если необходимо) описание причин, по которым такая информация требуется для соответствующей цели;

9.3.2 законное основание для обработки; и

9.3.3 сведения о хранении и удалении персональной информации в соответствии с нашей политикой или причинах отклонения от такой политики.

9.4 Мы обязуемся проводить регулярный анализ персональной информации, обработку которой мы выполняем, и актуализировать наши документы соответствующим образом.

10 Права субъектов данных

10.1 Субъекты данных обладают следующими правами в отношении их персональной информации:

10.1.1 право на получение сведений о том, каким образом, почему и на каких основаниях выполняется обработка информации – см. *[уведомлении о конфиденциальности и защите данных] компании Exide;*

10.1.2 право на получение подтверждения факта обработки их информации и право на осуществление доступа к такой информации и определенным видам других сведений на основании запроса;

10.1.3 право на уточнение данных в случае их недостоверности или неполноты;

10.1.4 право на удаление данных, если они более не требуются для цели, с которой они изначально были получены/обработаны, или при отсутствии законных оснований для обработки (данное право именуется «правом на забвение»);

10.1.5 право на ограничение объема обрабатываемой персональной информации в случае оспаривания достоверности информации или в случае незаконности обработки; и

10.1.6 право на временное ограничение объема обрабатываемой персональной информации, если субъект данных считает, что информация является недостоверной, или если субъект данных оспаривает право на ее обработку;

10.1.7 право на предоставление распоряжений о хранении, удалении и передаче их персональных данных после их смерти, если это требуется законодательством.

11 Обязательства субъектов данных

11.1 Физические лица обязаны содействовать Exide в актуализации своей персональной информации. Вы можете получить доступ к персональной информации других сотрудников, поставщиков и заказчиков в ходе выполнения ваших рабочих обязанностей или работы по договору подряда. В таком случае Компания ожидает, что вы поможете ей в соблюдении ее обязательств по защите данных перед субъектами данных. Если у вас имеется доступ к персональной информации, вы обязаны:

11.1.1 осуществлять доступ только к той персональной информации, с которой вы имеете право ознакомиться, исключительно в разрешенных целях;

11.1.2 позволять персоналу Exide осуществлять доступ к персональной информации только при наличии соответствующего разрешения;

11.1.3 позволять другим лицам, не являющимся сотрудниками Компании, осуществлять доступ к персональной информации только при наличии у вас соответствующего разрешения от Кадрового отдела или Юридического отдела;

11.1.4 обеспечивать безопасное хранение персональной информации (например, путем соблюдения правил контрольно-пропускного режима, доступа к компьютерам, защиты паролем и безопасного хранения и уничтожения файлов, а

также путем принятия других мер предосторожности согласно Глобальной политике обеспечения безопасности данных Компании);

11.1.5 брать с собой персональную информацию или устройства, содержащие персональную информацию (или устройства, которые могут осуществлять доступ к ней), за пределы помещений Компании только в том случае, если были приняты соответствующие меры защиты (например, псевдонимизация, шифрование или защита паролем) для обеспечения безопасности информации и устройства; и

11.1.6 не хранить персональную информацию на локальных жестких дисках или личных устройствах, используемых в рабочих целях.

11.2 Вы обязаны обратиться в Кадровый отдел или Юридический отдел, если вы уверены или считаете, что произошло (либо происходит или с большой долей вероятности произойдет) любое из следующего:

11.2.1 обработка персональных данных без законного основания для ее обработки, либо в случае обработки конфиденциальной персональной информации;

11.2.2 нарушение безопасности данных согласно приведенному далее пункту 15.1;

11.2.3 доступ к персональной информации без соответствующего разрешения;

11.2.4 небезопасное хранение или удаление персональной информации;

11.2.5 перемещение персональной информации или устройств, содержащих персональную информацию (или устройств, которые могут осуществлять доступ к ней), за пределы помещений Компании без принятия соответствующих мер защиты;

11.2.6 любое другое нарушение настоящей политики или принципов защиты данных согласно приведенному выше пункту 4.1.

12 Право субъектов данных на осуществление доступа

12.1 Субъект данных вправе подать запрос («Запрос на осуществление доступа») в любой момент времени, чтобы ознакомиться с информацией о персональных данных, которыми Компания владеет в отношении такого субъекта данных. Как правило, Компания обязана отвечать на Запросы на осуществление доступа в течение одного месяца с даты получения (в случае сложных и/или многочисленных запросов данный срок может быть увеличен до двух месяцев, и в такой ситуации субъекту данных будет сообщено о необходимости продления срока).

12.2 Все полученные запросы на осуществление доступа должны направляться местному Представителю по вопросам Общего регламента по защите данных.

12.3 Компания не взимает плату за обработку обычных Запросов на осуществление доступа. Exide вправе взимать дополнительные сборы в разумном объеме за подготовку дополнительных копий информации, которая уже была предоставлена субъекту данных, а также в отношении запросов, которые носят очевидно необоснованный или избыточный характер, особенно в случае многократной подачи одинаковых запросов.

13 Информационная безопасность

13.1 Компания будет принимать соответствующие технические и организационные меры для обеспечения безопасности персональной информации и ее защиты от несанкционированной или незаконной обработки, а также от случайной утраты, уничтожения или повреждения. Такие меры могут включать:

13.1.1 контроль псевдонимизации или шифрования персональной информации (при наличии такой возможности);

13.1.2 непрерывное обеспечение конфиденциальности, целостности, доступности и надежности систем и служб обработки данных;

13.1.3 обеспечение возможности своевременного восстановления персональной

информации в случае физических или технических инцидентов; и

13.1.4 процесс регулярной проверки, оценки и анализа эффективности технических и организационных мер обеспечения безопасности обработки.

13.2 Если Компания привлекает сторонние организации для обработки персональной информации от ее имени, в договорах с такими организациями должны быть предусмотрены дополнительные меры обеспечения безопасности персональной информации. В частности, договоры со сторонними организациями должны предусматривать, что:

13.2.1 организация вправе действовать исключительно на основании распоряжений Exide;

13.2.2 организации, выполняющие обработку данных, должны принять на себя обязательство по сохранению конфиденциальности;

13.2.3 для обеспечения безопасной обработки должны быть приняты соответствующие меры;

13.2.4 субподрядчики могут быть привлечены исключительно на основании предварительного разрешения Exide на основании письменного договора;

13.2.5 организация будет содействовать Exide в предоставлении доступа субъектам данных и позволять им осуществлять права на защиту данных;

13.2.6 организация будет содействовать Exide в выполнении ее обязательств по обеспечению безопасности обработки, уведомлении о нарушении безопасности данных и оценке воздействия на защиту данных;

13.2.7 организация будет обязана удалить или вернуть всю персональную информацию Exide по ее запросу по завершении срока действия договора;

13.2.8 организация пройдет проверки и аудит, предоставить Exide любую информацию, которая потребуется Компании для обеспечения соблюдения обязательств по защите данных компанией Exide и организацией; и

13.2.9 организация будет обязана немедленно сообщать Exide о любых запросах на осуществление действий, нарушающих законодательство в сфере защиты данных.

13.3 Перед заключением нового соглашения об обработке персональной информации сторонней организацией или изменением действующего соглашения соответствующие сотрудники должны обратиться в Юридический отдел для утверждения условий такого соглашения.

14 Хранение персональной информации

14.1 Персональная информация (и конфиденциальная персональная информация) будет храниться безопасным образом в соответствии с Глобальной политикой обеспечения безопасности данных Компании.

14.2 Персональная информация (и конфиденциальная персональная информация) не будет храниться дольше, чем требуется. Продолжительность хранения данных будет зависеть от обстоятельств, включая причины, по которым был осуществлен сбор данных. Сотрудники должны соблюдать Политику хранения учетных документов Компании, в которой описывается срок хранения или критерии его определения. При наличии неопределенности сотрудники должны обращаться к местному Представителю по вопросам Общего регламента по защите данных или в Юридический отдел.

15 Нарушения безопасности данных

15.1 Нарушения данных бывают разными, например:

15.1.1 утрата или кража данных или оборудования, на котором хранится персональная информация;

15.1.2 несанкционированный доступ или использование персональной

информации сотрудниками или третьими сторонами;

15.1.3 утрата данных в результате неисправности в оборудовании или системах (включая аппаратные и программные средства);

15.1.4 человеческий фактор (например, случайное удаление или изменение данных);

15.1.5 непредвиденные обстоятельства (такие, как пожар или наводнение);

15.1.6 умышленные атаки на информационные системы (например, атаки хакеров, повреждение вирусами или фишинговыми программами); и

15.1.7 получение информации у хранящей ее организации обманным путем.

15.2 Компания обязуется:

15.2.1 без необоснованных задержек направлять соответствующий отчет о нарушениях безопасности данных в соответствующий Орган надзора или в Управление Комиссара по информации (Соединенное Королевство), по возможности – в течение 72 часов с момента, когда ей становится известно о нарушении, если оно может поставить под угрозу права и свободы субъектов данных; и

15.2.2 уведомлять заинтересованных субъектов данных о нарушении безопасности данных, если оно с высокой долей вероятности поставит под угрозу их права и свободы, а также в случаях, когда уведомление требуется по закону.

16 Передача в другие страны

16.1 Компания может передавать персональную информацию за пределы Европейской Экономической Зоны (ЕЭЗ) (в которую входят страны Европейского Союза и Исландия, Лихтенштейн и Норвегия) своей материнской компании, Exide Technologies, расположенной в США, ввиду того, что в Exide Technologies применяются стандартные меры по защите данных.

17 Обучение

Компания обязуется обеспечить надлежащее обучение персонала его обязанностями по защите данных. Лица, чьи должностные обязанности требуют регулярного осуществления доступа к персональной информации, или лица, ответственные за реализацию данной политики или работа с запросами субъектов данных в рамках настоящей политики, пройдут дополнительное обучение, которое поможет им понять и выполнять свои обязанности.

18 Последствия несоблюдения

18.1 Компания очень серьезно относится к соблюдению данной политики. Несоблюдение настоящей политики:

18.1.1 ставит под угрозу субъектов данных, персональная информация которых подвергается обработке; и

18.1.2 создает риск значительных санкций по гражданскому и уголовному праву для отдельных лица и Компании в целом; и

18.1.3 в некоторых обстоятельствах может быть расценено как уголовное преступление, совершенное отдельным лицом.

18.2 Учитывая важность данной политики, несоблюдение сотрудником любых приведенных здесь требований может привести к дисциплинарным взысканиям, предусмотренным нашими процедурами, включая увольнение за грубый проступок. В случае нарушения данной политики лицом, не являющимся сотрудником, договор с ним может быть немедленно расторгнут.

18.3 Если у вас имеются вопросы или сомнения в связи с данной политикой, не стесняйтесь обращаться к Общенациональному представителю по вопросам Общего регламента по защите данных или к сотрудникам Юридического отдела.