



**Сеть Международного движения Красного Креста и Красного
Полумесяца по восстановлению семейных связей
Кодекс поведения в отношении
защиты данных**

Версия 1.0

Ноябрь 2015

Предисловие

Настоящий Кодекс поведения (КП) был составлен рабочей группой, состоящей из представителей Австрийского Красного Креста (Клара Шохер-Дёринг), Бельгийского Красного Креста (Фландрия) (Аксель Ванде Вегате, Надя Терведуве), Британского Красного Креста (Марк Бейнем и Эмили Нокс), Красного Креста Германии (Ютта Херманнс), офиса Красного Креста при ЕС (Оливье Женар), Международного Комитета Красного Креста (Ромэн Бирхер, Массимо Марелли, Катя Гизин) и Международной Федерации обществ Красного Креста и Красного Полумесяца (Кристофер Расси) (Рабочая группа). Некоторые другие представители этих организаций также принимали участие в составлении текста, в обсуждениях и заседаниях, что явилось важным вкладом в работу. Рабочая группа приступила к обсуждению проекта в конце 2013 г. и кроме многочисленных телеконференций и обмена сообщениями по электронной почте провела несколько рабочих заседаний в Мехелене (апрель 2014 г.), Брюсселе (июль 2014 г.), Вене (сентябрь 2014 г.), Софии (ноябрь 2014 г.) и Лондоне (январь 2015 г.). КП был принят Рабочей группой на основе консенсуса и с учетом информации, полученной от многочисленных национальных обществ.

Было решено, что КП необходим в силу (1) большого числа акторов Международного Движения Красного Креста и Красного Полумесяца (Движения), осуществляющих деятельность в Сети по восстановлению семейных связей, и необходимости передавать данные в рамках Движения и внешним акторам, а также в силу (2) изменяющейся ситуации с нормативно-правовой регламентацией в Европе и во всем мире в том, что касается законов и стандартов в области защиты данных. В КП излагается минимум принципов, обязательств и процедур, которые члены Движения должны выполнять при обработке данных в Сети по восстановлению семейных связей. В КП отражено стремление соблюдать наиболее строгие нормативные положения по защите данных, особенно законодательство Европейского Союза в этой области. Пользователи КП должны также обеспечить соблюдение их собственного национального законодательства. КП является справочным документом, интегрированным в основной комплекс директивных указаний Движения по вопросу восстановления семейных связей (ВСС). Членам Движения нужно принять настоящий кодекс, который должен найти отражение в их собственных стандартных процедурах.

Настоящий КП даст всем членам Движения один инструмент, который можно использовать для защиты основных прав и свобод отдельных лиц, в частности, права на неприкосновенность личной жизни и защиту личных данных, которые обрабатываются в ходе деятельности по ВСС. Хочется надеяться, что КП будет способствовать установлению доверия к работе Движения как среди отдельных лиц, так и законодателей, а также членов Движения, которые должны передавать друг другу данные по делам, связанным с ВСС.

ОПРЕДЕЛЕНИЯ

Международное движение Красного Креста и Красного Полумесяца (Движение)

Движение является всемирным гуманитарным движением, задача которого заключается в том, чтобы «предотвращать и облегчать страдания людей, защищать жизнь и здоровье человека и обеспечивать уважение к человеческой личности, особенно во время вооруженных конфликтов и других чрезвычайных ситуаций, заниматься деятельностью по профилактике заболеваний, развитию здравоохранения и социального обеспечения, поощрять добровольную работу, содействовать тому, чтобы члены Движения всегда были готовы к оказанию помощи, и крепить всеобщую солидарность с теми, кто нуждается в помощи и защите со стороны Движения».

Международный Комитет Красного Креста (МККК), национальные общества Красного Креста и Красного Полумесяца (национальные общества) и Международная Федерация обществ Красного Креста и Красного Полумесяца (МФОКК и КП) являются составными частями Движения.

Центральное агентство по розыску (ЦАР)

Центральное агентство по розыску (ЦАР) является постоянно действующей службой в составе МККК в соответствии с положениями четырех Женевских конвенций и Дополнительных протоколов к ним, а также Уставом Движения. ЦАР, сотрудничая с другими составными частями Движения, осуществляет деятельность по восстановлению семейных связей (ВСС) во время вооруженных конфликтов и других ситуаций насилия, катастроф и иных обстоятельств, которые требуют реакции со стороны гуманитарных организаций. Согласно Севильскому соглашению 1997 г., Дополнительных мер к нему 2005 г. и Стратегии Движения в области ВСС на период с 2008 по 2018 гг. ЦАР играет ведущую роль в рамках Движения при решении всех вопросов, касающихся ВСС; оно координирует действия и является техническим консультантом национальных обществ.

Оператор данных

Оператор данных – это любая составная часть Движения, которая самостоятельно или совместно с другими определяет цели и средства обработки персональных данных.

Обработчик данных

Обработчик данных это лицо, орган государственной власти, агентство или другой орган, который обрабатывает персональные данные от имени оператора данных.

Координатор действий по защите данных при ВСС

Координатор действий по защите данных при ВСС это лицо или подразделение, которое отвечает за обеспечение соблюдения КП.

Субъект данных

Субъект данных это физическое лицо (т.е. индивидуум), которого можно идентифицировать, прямо или косвенно, на основании персональных данных.

Для того чтобы определить, является ли лицо опознаваемым, необходимо принять во внимание все средства, которые, как можно предположить на разумных основаниях, могут быть использованы либо оператором, либо любым лицом для идентификации человека прямо или косвенно. Для установления того, будут ли средства, исходя из разумных предположений, использоваться для идентификации лица, необходимо принять во внимание все объективные факторы, такие как стоимость и объем времени, требуемого для идентификации, принимая во внимание как имеющуюся во время обработки технологию, так и развитие в области технологии. Персональные данные поэтому не включают анонимную информацию, которая не имеет отношения к определенному или поддающемуся определению физическому лицу, или данные, превращенные в анонимные таким образом, что субъект данных более не является идентифицируемым. Данный КП не касается поэтому обработки такой анонимной информации, в том числе для целей статистики и научных исследований.

При использовании онлайн-сервисов отдельные лица могут ассоциироваться с онлайн идентификаторами, предоставляемыми их устройствами, приложениями, инструментами и протоколами, такими как адреса Интернет протокола или cookies (идентификационные файлы, сохраняемые на клиентской системе). Это может оставлять следы, которые в сочетании с уникальными идентификаторами и другой информацией, полученной серверами, могут быть использованы для описания отдельных лиц и их идентификации. Номера, данные о местонахождении, онлайн идентификаторы (например, IP-адреса или cookies) и другие конкретные элементы как таковые не должны считаться персональными данными, если они не определяют лицо и не делают это лицо определяемым.

Члены семьи

Лица, которые считаются членами семьи, это, по крайней мере:

- дети, рожденные в браке и вне брака, приемные дети и дети одного из родителей;
- партнеры, как в зарегистрированном браке, так и вне его;
- родители, включая родителей мужа или жены и приемных родителей;
- братья и сестры, рожденные от одних родителей или разных родителей, и приемными;
- близкие родственники¹

¹ Во многих социо-культурных контекстах семья может включать всех тех лиц, которые проживают под одной крышей или поддерживают между собой тесные отношения. Таким образом, понятие семьи следует

Определение, которое можно обнаружить в национальном законодательстве, также должно быть принято во внимание.

Несовершеннолетние

Любой человек, не достигший возраста восемнадцати лет, если в соответствии с законодательством, применимым к ребенку, совершеннолетие не наступает раньше.

Другие лица

Кроме запрашивающего или разыскиваемого лица деятельность по ВСС может касаться других лиц, например, членов семьи, свидетелей, соседей, руководителей общин, других разыскиваемых лиц и т.д.

Персональные данные

Персональные данные означают любую информацию об определенном или поддающемся определению физическом лице. Поддающимся определению физическим лицом является лицо, которое может быть идентифицировано, прямо или косвенно, в частности, исходя из таких идентификаторов, как имя, аудио-визуальный материал, число, данные о местонахождении, онлайн идентификатор, или одного или нескольких факторов, характерных для физической, психологической, генетической, психической, экономической, культурной или социальной идентичности этого лица.

Персональные данные не включают анонимной информации, т.е. информации, которая: а) не относится к определенному или поддающемуся определению физическому лицу; или б) которая превратилась в анонимную таким образом, что субъект данных более не может быть определен.

Компрометация персональных данных

Компрометация персональных данных означает нарушение правил обеспечения безопасности, приводящее к тому, что передаваемые, хранящиеся или иным образом обрабатываемые персональные данные могут быть случайно или незаконно уничтожены, утрачены, изменены, несанкционированно преданы гласности и стать доступными или подвергнуться такой опасности.

Обрабатывать/Обработка / Обработанные

Термины «обрабатывать/ обработка/ обработанные» относятся к любой операции или набору операций, которые осуществляются с персональным данными или комплексом персональных данных как при помощи автоматизированных средств, так и нет. Это сбор, регистрация, организация, структурирование, хранение, адаптация или изменение, восстановление, использование, раскрытие путем передачи, распространение или иным образом обеспечение доступности, а также уничтожение данных. Передача данных в рамках Движения или за его пределы является операцией по обработке.

Основные этапы обработки

Основные этапы обработки являются ключевыми шагами процедуры. Эти этапы должны быть задокументированы операторами данных и включать:

- дату и источник сбора данных;
- если правовым основанием для обработки является согласие, любые ограничения на это согласие, выраженные субъектом данных;
- дату, тип и результат запроса субъекта данных на осуществление прав субъекта данных;
- дату передачи и получателя любых данных;
- дату и средство публикации;
- оценку эффективности защиты данных (ОЭЗД), если она осуществлялась;
- закрытие файла;
- архивирование, если уместно.

Получатель

Получатель – это лицо, орган государственной власти, агентство или другое образование, не являющееся субъектом данных, оператором данных или обработчиком данных, которому предоставляются персональные данные.

Деятельность по восстановлению семейных связей и деятельность, связанная с восстановлением семейных связей

Восстановление семейных связей (ВСС) является общим термином, описывающим диапазон видов деятельности, направленной на предотвращение разделения членов семей, оказание им помощи в восстановлении и поддержании связи, а также деятельность, осуществляемая с целью выяснения участи и местонахождения лиц, пропавших без вести.

Такая деятельность может быть связана с другими услугами по оказанию поддержки, например, предоставлением психологической и психосоциальной, юридической, административной и материальной помощи семьям и другим пострадавшим лицам, а также с программами по переселению и реинтеграции и услугами по социальному обеспечению (подробности см. в Приложении 1)

Услуги по ВСС

Национальные общества и делегации МККК во всем мире выделяют сотрудников в рамках своих структур, которые разрабатывают и осуществляют деятельность по ВСС и связанную с этой деятельностью.

Сеть Движения по восстановлению семейных связей

Когда члены семьи разлучены и люди пропадают без вести в результате вооруженного

конфликта или других ситуаций насилия, катастроф, миграции или иных гуманитарных кризисов, должно быть сделано все возможное, чтобы установить их участь и местонахождения, восстановить связь между ними и, если целесообразно, воссоединить их.

Службы национальных обществ и МККК по ВСС составляют единую всемирную сеть, которая называется **«Сеть по восстановлению семейных связей»**. ЦАР выступает в роли технического советника и координатора этой Сети по восстановлению семейных связей. Сила этой гуманитарной сети заключается в ее возможности мобилизовать сотрудников и добровольцев во всем мире и работать в соответствии с едиными принципами и по единой методике в областях, пострадавших от вооруженных конфликтов, других ситуаций насилия, катастроф, миграции и иных гуманитарных кризисов, пересекая границы.

Дополнительную информацию о Сети по восстановлению семейных связей можно получить на сайте по адресу: <http://familylinks.icrc.org>.

Уязвимое лицо

Уязвимым лицом в контексте настоящего КП является любой человек с пониженной способностью выразить свободно и конкретно свои обоснованные желания либо из-за i) эмоционального и психологического воздействия разделения семьи и влияющих на него гуманитарных обстоятельств, либо из-за ii) сложности требуемой обработки, что затрудняет для него полное понимание связанных с этим опасностей и (или) преимуществ, или и того, и другого одновременно.

Введение

1.1 Цель настоящего Кодекса поведения (КП)

В настоящем КП излагается минимум принципов, обязательств и процедур, которые сотрудники по ВСС МККК, национальных обществ и МФОКК и КП должны выполнять при обработке данных в ходе деятельности по ВСС для того, чтобы: 1) соблюдать применимые стандарты и законодательство в области защиты данных; 2) обеспечить беспрепятственную передачу данных, необходимых для ВСС и 3) защитить основные права и свободы заявителей, разыскиваемых лиц и других лиц, таких как свидетели или иные члены семьи, связанные с деятельностью по ВСС согласно международному гуманитарному праву (МГП), международному праву прав человека и другим международным стандартам, в частности права на неприкосновенность частной жизни и на защиту персональных данных.

1.2 Сфера применения настоящего КП

1.2.1 Восстановление семейных связей

Настоящий КП применяется к деятельности операторов данных по ВСС и их деятельности, связанной с ВСС (см. Приложение 1).

1.2.2 Персональные данные

Настоящий КП применяется к обработке персональных данных (включая данные, касающиеся умерших лиц), осуществляемой операторами данных в отношении запрашивающих и разыскиваемых лиц, и других лиц, которых касается деятельность по ВСС.

1.3 *Сеть по восстановлению семейных связей*

Конвенции 1949 г., Дополнительные протоколы к ним 1977 г., Устав Международного движения Красного Креста и Красного Полумесяца (Устав Движения), резолюции, принятые Советом делегатов и резолюции Международной конференции Красного Креста и Красного Полумесяца предоставляют операторам данных мандат на осуществление деятельности по ВСС.

Национальные общества выполняют этот мандат в качестве вспомогательных органов своих соответствующих государственных властей в гуманитарной области и по всему миру играют уникальную роль в области ВСС. Они организуют вместе с государственными властями различные службы по оказанию помощи жертвам вооруженных конфликтов, стихийных бедствий и других чрезвычайных ситуаций, которые нуждаются в помощи.

1.4 *Принципы и директивные указания Движения*

1.4.1 Основопологающие принципы

Операторы данных осуществляют свою деятельность в соответствии с Основопологающими принципами, которыми руководствуется Движение: гуманность, беспристрастность, нейтральность, независимость, добровольность, единство и универсальность. Вся обработка персональных данных, осуществляемая в ходе деятельности по ВСС операторами данных должна, соответствовать этим принципам.

1.4.2. «Не навреди»

Предоставляя услуги по ВСС, операторы данных делают все возможное для того, чтобы избежать причинения вреда людям при обработке персональных данных.

1.4.3 Конфиденциальность или правила разглашения

Если субъекты данных предоставляют информацию операторам данных на условиях конфиденциальности, операторы данных должны уважать эти условия и обеспечить защиту этой информации.

Операторы данных должны выполнять все применимые национальные, региональные и международные правовые обязательства при соблюдении ограничений, описанных в данном разделе 1.4. При определении применимости таких обязательств ссылка делается на: 1) любые привилегии и иммунитеты или освобождение от обязательств, которыми пользуются операторы данных в конкретной стране или конкретном регионе; и 2) любые правовые нормы защиты, вытекающие из международного права, включая МГП, и мандат, выданный в соответствии с Уставом Движения.

1.4.4 Действующие Руководства

Обработка персональных данных осуществляется в соответствии с Руководствами, касающимися деятельности по ВСС Сети по восстановлению семейных связей, такими как «Восстановление семейных связей. Руководство для национальных обществ Красного Креста и Красного Полумесяца»², «Оценка потребностей в области восстановления семейных связей. Руководство для национальных обществ и МККК», «Восстановление семейных связей при стихийных бедствиях и катастрофах. Практическое руководство» и «Руководство по предоставлению услуг в области восстановления семейных связей лицам, разлученным в результате миграции»³, а также в соответствии с Профессиональными стандартами работы по предоставлению защиты⁴.

² Пересматривается

³ Соответствующие документы можно найти на русском или английском языке в сети Family Links Extranet (в разработке).

⁴ <https://www.icrc.org/eng/resources/documents/publication/p0999.htm>

2. Основные принципы обработки и обязательства оператора данных

2.1 Точно определенная цель

Во время сбора данных оператор данных должен определить и изложить конкретную, ясную и законную цель (или цели), для которой обрабатываются данные.

Обработка данных в первую очередь осуществляется с гуманитарной целью восстановить семейные связи между людьми, разделенными в результате вооруженного конфликта, других ситуаций насилия, катастроф, миграции или иных ситуаций, требующих реакции со стороны гуманитарных организаций.

Данные могут обрабатываться для иных целей, нежели те, которые изначально указывались во время сбора данных, если дальнейшая обработка необходима для гуманитарных целей, таких как деятельность, связанная с ВСС, и будет неизменно соответствовать всем законам, касающимся защиты данных (более подробно см. Приложение 1).

2.2 Законная и справедливая обработка данных

Обработка персональных данных оператором данных основывается на одном или нескольких из перечисленных ниже факторов.

- Согласие субъекта данных.
- Жизненно важный интерес субъекта данных или других лиц.
- Общественный интерес.
- Законный интерес оператора данных.
- Выполнение юридического обязательства.

2.2.1 Согласие субъекта данных

Согласие является предпочтительным выбором: согласие субъекта данных является предпочтительной основой для обработки персональных данных. Согласие должно быть дано однозначно любым соответствующим способом, позволяющим свободно выразить конкретное и обоснованное желание субъекта данных в форме письменного, устного или выраженного иным способом заявления либо посредством четкого позитивного действия субъекта данных, означающего его согласие на обработку его персональных данных. Согласие относится ко всем видам деятельности по обработке, осуществляемым с одной целью. Субъект данных должен получить следующую информацию на понятном языке:

- личность и контакты оператора данных;
- конкретная цель обработки его персональных данных и разъяснение возможных рисков и преимуществ;
- тот факт, что оператор данных может обрабатывать его персональные данные для целей иных, нежели те, которые были заявлены во время сбора данных, если это не противоречит конкретной цели, упомянутой выше;
- обстоятельства, при которых может отсутствовать возможность работать с персональными данными конфиденциально;
- права субъекта данных и ограничения на его право доступа, право исправлять или стирать (уничтожать) его персональные данные и позже возражать против обработки;
- меры безопасности, принимаемые оператором данных в связи с обработкой данных;
- оператору данных может потребоваться передать данные в другую страну;
- политика оператора данных относительно их сохранения (как долго записи сохраняются и любые шаги, предпринимаемые для обеспечения правильности данных и их обновления);
- могут ли данные предоставляться другим организациям (в том числе, другим составным частям Движения), органам государственной власти страны, где данные собирались, или другой страны и могут ли они разглашаться.

Субъекты данных должны дать согласие на использование их персональных данных таким образом.

Согласие может быть предоставлено на определенных условиях. Подробности данного согласия, требующийся уровень конфиденциальности и любые применимые ограничения регистрируются и хранятся вместе с персональными данными в ходе всего процесса обработки.

Альтернативные варианты – особенно когда согласие не может быть получено или его получение практически трудноосуществимо, персональные данные обрабатываются на одном

из следующих оснований:

- жизненно важный интерес;
- общественный интерес;
- законный интерес оператора данных;
- выполнение юридической обязанности.

В этом случае оператор данных постарается обеспечить, если это возможно, осведомленность субъекта данных о такой обработке и его возможность возражать против обработки, если он пожелает.

2.2.2 Жизненно важный интерес

Предполагается, что обработка персональных данных службами ВСС оператора данных, осуществляемая с целью восстановления семейных связей, выяснения участи и местонахождения лиц, пропавших без вести, и предоставления срочной помощи и защиты, соответствует жизненно важным интересам субъекта данных или других лиц при определенных обстоятельствах, а именно:

- когда субъект данных разыскивается родственниками, объявлен пропавшим без вести, лишен свободы, стал жертвой преступления или считается умершим;
- когда субъект данных является особенно уязвимым и/или не может свободно предоставить обоснованное согласие либо предвидеть и понимать опасности и преимущества обработки своих персональных данных.

2.2.3 Общественный интерес

Деятельность по ВСС и связанная с ней деятельность оператора данных соответствуют общественным интересам, поскольку она имеет исключительно гуманитарный характер, как указывается в разделе 1.3 выше. (Например, см. Приложение 2)

2.2.4 Законный интерес

Персональные данные обрабатываются также в обстоятельствах, когда это соответствует законным интересам оператора данных, и при условии, что интересы и основные права и свободы субъекта данных не имеют преимущественной силы над законными интересами (например, см. Приложение 3).

2.2.5 Выполнение юридической обязанности

Кроме того, оператор данных будет обрабатывать персональные данные в соответствии с любой применимой юридической обязанностью, например, для выполнения требований национального или регионального законодательства и судебных постановлений, при условии соблюдения основополагающих принципов Движения. Юридические обязанности могут быть разными в различных странах и в различных ситуациях.

2.3 Обязательства в области обработки данных

2.3.1 Ответственность / Подотчетность

Оператор данных должен гарантировать, что любое лицо или образование, которые имеют доступ к персональным данным и действуют в соответствии с его инструкциями (являясь поэтому обработчиками данных) не будут обрабатывать эти персональные данные кроме как методами, соответствующими настоящему КП. Оператор данных также должен обеспечить четкое распределение обязанностей всех образований, участвующих в обработке персональных данных, что должно быть отражено в соответствующих положениях контракта. См. раздел 4 далее, где дается дополнительная информация о передаче данных третьим сторонами, если предполагается, что получающая их третья сторона не будет обрабатывать данные исключительно в соответствии с указаниями оператора данных.

2.3.2 Обработка достоверных, имеющих отношение к делу и уточнённых данных

Достоверные данные – персональные данные, обрабатываемые службами ВСС оператора данных, должны пересматриваться для обеспечения того, что они достоверны, имеют отношение к делу и не являются чрезмерными для целей, в которых они собираются и обрабатываются, за исключением случаев, когда они архивируются.

Точность данных – персональные данные должны быть достаточно точными, полными и обновленными для тех целей, в которых они собираются и обрабатываются.

2.3.3 Защита данных путем специально разработанных мер и по умолчанию

Соответствующие технические и организационные меры должны быть приняты для удовлетворения требований настоящего КП при разработке систем управления данными и создания процедуры для сбора персональных данных.

2.3.4 Оценка эффективности защиты данных (ОЭЗД)

Если обработка данных, например, передача, опубликование и разглашение, может представлять собой конкретную опасность для прав и свобод субъекта данных, оператор данных до начала обработки проведет ОЭЗД при консультациях с субъектом данных и другими заинтересованными сторонами, если это возможно, для того, чтобы определить и оценить, в частности:

- преимущества обработки данных;
- причины, характер, вероятность и степень рисков;
- соответствующие меры, которые должны быть приняты для того, чтобы продемонстрировать, что уровень рисков минимизирован и обработка персональных данных осуществляется в соответствии с настоящим КП и любыми применимыми нормами права.

Результатом ОЭЗД должна быть минимизация опасности причинения вреда/или возможного

посягательства на права и свободы субъекта данных. Оператор данных документирует результат и причины, по которым этот результат был получен. Оператор данных обеспечивает также должное осуществление мер, принятых по итогам ОЭЗД, и достижение планируемого эффекта.

2.3.5 Документирование обработки данных

Оператор данных обеспечивает сохранение данных в электронном или бумажном виде с указанием: i) базы данных, в которых осуществляется обработка персональных данных, и ii) основных этапов процесса обработки данных. Эти этапы регистрируются в базе данных/индивидуальном файле субъекта данных.

2.3.6 Сохранение данных

Персональные данные будут заархивированы или уничтожены в соответствии с политикой оператора данных в области сохранения данных службами ВСС, если эти данные более не нужны для целей, в которых они собирались, для дальнейшей обработки или для обработки на других законных основаниях (см. также раздел 3.3).

2.3.7 Безопасность данных

Разумные технические, физические и организационные меры безопасности должны приниматься на любом этапе обработки данных для защиты персональных данных от утраты, кражи, несанкционированного или незаконного доступа или разглашения. Доступ к персональным данным ограничен и предоставляется только сотрудникам оператора данных, которым требуется такой доступ для предоставления конкретной услуги или выполнения конкретной задачи (подробнее см. Приложение 4).

2.3.8 Компрометация персональных данных

Оператор данных уведомляет субъекта данных о том, что имела место компрометация персональных данных, если это может повлиять на права и свободы субъекта данных.

Уведомления субъекта данных о нарушениях направлены на то, чтобы свести к минимуму опасность их отрицательного воздействия на субъекта данных.

Оператор данных может принять решение, что сообщения субъекту данных о компрометации персональных данных не требуется, если имеет место что-либо из следующего:

- оператор данных принял должные организационные, технические или физические меры по защите, и эти меры были применены в отношении данных, которых касается компрометация;
- оператор данных принял последующие меры, которые гарантируют, что более не существует опасности того, что права и свободы субъекта данных могут серьезно пострадать;
- это потребует несоразмерных усилий, в частности, в силу существующих логистических условий или условий безопасности, либо из-за числа подобных

случаев; в таких обстоятельствах оператор данных рассмотрит возможность обратиться с публичным заявлением или принять аналогичные меры, посредством которых субъекты данных будут проинформированы в равной степени эффективно;

- это будет иметь пагубные последствия для общественных интересов, в том числе, для действий оператора данных;
- установление контакта с субъектом данных в силу существующих условий безопасности может подвергнуть опасности самого субъекта данных.

3. Права субъектов данных

3.1 Информация и доступ

При сборе персональных данных или как можно скорее после его окончания оператор данных предоставляет субъекту данных, учитывая ограничения, связанные с логистикой и обеспечением безопасности, информацию об обработке его персональных данных устно или в письменной форме, используя наиболее подходящие средства (перечень пунктов информации, которая должна быть предоставлена, см. в Приложении 5).

Субъекты данных имеют право получить в любое время по требованию подтверждение того, обрабатываются ли касающиеся их персональные данные. Если такие персональные данные действительно обрабатываются, они имеют право получить доступ к своим персональным данным и к информации о цели обработки, получателях персональных данных и принятых мерах безопасности.

По требованию предоставляется копия документа (документов), содержащего(их) их персональные данные.

Данный раздел не применим, если доступ к данным должен быть ограничен по причине:

- важнейшего общественного интереса;
- интересов в области защиты данных и прав и свобод других;
- того, что соответствующие документы не могут быть отредактированы с сохранением смысла.

Оператор данных регистрирует запросы на доступ и результаты таких запросов, в том числе, категории раскрытых персональных данных и/или отказы в доступе к информации.

3.2 Раскрытие информации для членов семьи и опекунов

Предполагается, что запрос о предоставлении персональных данных, поступивший от члена семьи или законного опекуна ребенка или другого субъекта данных, который не может предоставить согласия из-за недееспособности, соответствует наилучшим интересам этого лица и поэтому удовлетворяется, если нет достаточных причин предполагать иное. С лицом, которого это касается, следует проконсультироваться, если возможно, чтобы понять, не

возражает ли он против такого раскрытия данных.

3.3 Исправление и удаление

Исправление – оператор данных должен удовлетворить просьбу об исправлении персональных данных, особенно если данные неточные или неполные. Оператор данных сообщает о внесенных исправлениях получателям персональных данных, если только исправления не являются незначительными или если такое сообщение не связано с несоразмерными усилиями.

Удаление – субъект данных имеет право на удаление своих персональных данных из активных баз данных оператора данных в любом из следующих случаев:

- его персональные данные более не нужны для целей, в которых они собирались, или они не нужны для дальнейшей обработки;
- субъект данных отозвал свое согласие на обработку, и нет других оснований для обработки его персональных данных;
- субъект данных возражает против обработки его персональных данных;
- обработка персональных данных субъекта данных иным образом не соответствует настоящему КП.

Однако продолжение сохранения персональных данных субъекта данных допустимо, если это необходимо или оправдано:

- в силу исторических, статистических или научных целей, например, для документирования действий, предпринимаемых оператором данных при исполнении его мандата в соответствии с Женевскими конвенциями 1949 г., Дополнительными протоколами к ним 1977 г. и (или) Уставом Движения;
- по причинам общественного интереса в области общественного здравоохранения; или
- для публикации каким-либо лицом журналистского, литературного или художественного материала в осуществление права на свободу выражения и информации.

Более того, продолжение сохранения персональных данных субъекта данных разрешается, если это требование закона. Субъект данных должен быть уведомлен о решении, принятом по его запросу, что будет зарегистрировано оператором данных.

Оператор данных оставляет за собой право не удовлетворять запрос субъекта данных об исправлении или удалении, если он считает, что субъект данных, возможно, сделал запрос под давлением и (или) если удаление может пагубно сказаться на жизненно важных интересах субъекта данных.

Оператор данных сообщает об удалении персональных данных получателям и просит их удалить любые ссылки на такие данные или их копии, если только удаленные данные не являются незначительными или если сообщение не требует несоразмерных усилий.

3.4 Возражение против обработки

Субъект данных имеет право возражать на разумных основаниях, связанных с его конкретной ситуацией, против обработки его персональных данных, основанием для которой служит законный интерес оператора данных или общественный интерес. Если возражение принимается, соответствующие персональные данные более не обрабатываются при условии, что оператор данных не продемонстрирует важнейших законных оснований для продолжения обработки.

Если возражение принято, оператор данных сообщает о таком возражении получателям данных, если это не связано с несоразмерными усилиями.

3.5 Процедура

Субъект данных направляет свой запрос оператору данных, который дает ответ в течение разумного периода времени и в любом случае в течение периода времени, предусматриваемого законом.

Сотрудники, получающие просьбу от субъекта данных:

- либо соглашаются удовлетворить просьбу и уведомляют запрашивающее лицо о том, каким образом она была или будет удовлетворена; либо
- информируют запрашивающего субъекта данных, почему просьба не будет или не может быть удовлетворена; и
- информируют субъекта данных о возможности подать жалобу оператору данных.

4. Особое положение о передаче данных

4.1 Общие принципы

4.1.1 Информация общего характера

ВСС и деятельность, связанная с ВСС, часто требуют передачи персональных данных через границу между операторами данных.

Услуги по ВСС оператора данных также могут потребовать передачи персональных данных таким образованиям, как неправительственные организации (НПО), международные организации, органы власти и другие третьи стороны, нужные для осуществления ВСС и связанной с ВСС деятельности.

Такие передачи имеют место в соответствии с деятельностью Сети по восстановлению семейных связей, как это и излагается в разделе 1.3; как таковые они осуществляются по важным основаниям – общественный интерес, а также принципы и руководящие указания Движения, изложенные в разделе 1.4.

Кроме того, в большинстве случаев эти передачи осуществляются на основании согласия и (или) для защиты жизненно важных интересов субъекта данных или других лиц.

4.1.2 Общие принципы передачи данных

Передача данных в рамках Движения или за его пределы составляет операцию по обработке данных. Как таковая она должна соответствовать Основополагающим принципам, изложенным в Главе 2, и правам субъектов права, изложенным в Главе 3. Передача является, однако, особенно сложной операцией по обработке данных. Поэтому особенно важны некоторые требования к обработке данных, например, проведение ОЭЗД, информирование субъекта данных и обеспечение безопасности данных.

Как установлено в разделе 3.1 выше, передача всем возможным третьим сторонам предусматривается до/ во время сбора данных, и, по возможности, получается согласие субъекта данных на передачу его персональных данных.

Персональные данные не должны передаваться людям или организациям, если не работают соответствующие и соразмерные меры предосторожности, учитывающие деликатный характер данных, срочность гуманитарных действий и ограничения логистического порядка и связанные с обеспечением безопасности, как подробно излагается в настоящем КП.

4.1.3 Оценка эффективности защиты данных для передачи данных

Требование о проведении ОЭЗД является особенно важным в контексте передачи данных. Поэтому если передача данных может представлять собой особые риски для прав и свобод субъектов данных, оператор данных проводит ОЭЗД (см. Приложение 6) до передачи, как это установлено в разделе 2.3.4 выше.

4.1.4 Условия

Передача данных должна соответствовать следующим условиям в совокупности:

- обработка данных получателем строго ограничена конкретными целями ВСС и связанной с ВСС деятельностью и согласующимися с ними целями;
- объем и тип персональных данных строго ограничены потребностями получателя для достижения указанных целей или предполагаемой дальнейшей обработки;
- передача соответствует обоснованным ожиданиям субъекта данных.

4.1.5 Документация передач данных

Оператор данных обеспечивает сохранность электронных регистрационных записей или регистрационных записей на бумажных носителях (см. также 2.3.5).

Регистрационные записи передачи должны содержать все следующие пункты:

- имя получателя;
- конкретную цель передачи;
- дату передачи;

- описание категорий персональных данных, которые были переданы;
- любые ограничения на использование данных, согласованные с получателем.

4.1.6 Соглашения

Как указано в разделе 4.1.2, передача персональных данных может состояться, если оператор данных убедился в существовании должных мер предосторожности в том, что касается защиты данных со стороны получателя. Должные меры предосторожности могут определяться посредством соглашений, касающихся обращения с персональными данными, которые заключаются, если это возможно, с третьими сторонами за пределами Движения всегда, когда рассматривается регулярная передача данных.

Даже когда соглашения заключены, может оказаться нецелесообразным передавать некоторые категории данных.

4.2 Методы передачи

В случае передачи используются соответствующие меры для обеспечения защиты передачи персональных данных третьим сторонам. Уровень безопасности и метод передачи должен соответствовать характеру и конфиденциальности персональных данных и рискам, выявленным в ходе ОЭЗД.

5. Особые положения, касающиеся публикации данных

5.1 Общие принципы

Публикация персональных данных оператором данных составляет операцию по обработке. Как таковая она должна соответствовать общим принципам, изложенным в Главе 2 и правам субъектов данных, указанным в Главе 3. Однако публикация является особенно деликатной операцией по обработке. Когда она имеет место, оператор данных и субъект данных утрачивают в значительной степени способность контролировать то, как персональные данные обрабатываются. Поэтому должны соблюдаться и дополнительные принципы, изложенные в настоящей главе.

В соответствии с результатами ОЭЗД и применимыми юридическими обязательствами, службы по ВСС оператора данных могут публиковать персональные данные, чтобы восстановить семейные связи между лицами, разделенными в результате вооруженных конфликтов, других ситуаций насилия, стихийных бедствий и миграции. Такие данные могут включать имена, фотографии, статус (например, жив и здоров, ранен, умер, пропал без вести, перемещенное лицо) и могут опубличиваться в режиме онлайн, через СМИ, посредством плакатов, листовок и других подходящих средств.

В соответствии с разделом 2.2.1 согласие субъекта данных является предпочтительным основанием для публикации персональных данных

5.2 Оценка эффективности защиты данных для опубликования данных

Требование провести ОЭЗД, устанавливаемое в разделе 2.3.4 выше и в Приложении 6, является особенно важным в контексте публикации данных.

Кроме элементов, указанных в разделе 2.3.4 («Оценка воздействия защиты данных»), в контексте публикации данных ОЭЗД учитывает следующие элементы:

- национальные законы и нормативные положения, которые применимы к публикации данных;
- ситуацию с обеспечением безопасности, уважением прав человека и МГП и безопасность субъектов данных в конкретной стране;
- будет ли достаточным опубликовать анонимные/ сводные данные или необходимо опубликовать персональные данные, будут ли другие средства защиты личности субъектов данных способствовать достижению конкретной цели публикации (к таким другим средствам могут относиться, например, отсутствие указания на связь между фотографией и именем /особыми приметами/точным местонахождением);
- метод и условия публикации;
- возможность обеспечить соблюдение требования, касающиеся ограничения на дальнейшее использование третьими сторонами, которые могут захотеть использовать опубликованные данные;
- возможность указать точный период, во время которого определенные данные могут оставаться открытыми в конкретных медийных пространствах, метод уничтожения после достижения конкретной цели публикации;
- полезность и целесообразность публикации, устанавливаемые посредством периодической оценки, проводимой оператором данных;
- в контексте публичной информационной деятельности важность защитить уязвимых лиц от любопытства людей.

Если субъект данных является уязвимым лицом, должны быть приняты во внимание, где это целесообразно, дополнительные соображения, включая меры предосторожности для защиты конфиденциальности и анонимности. Руководящим принципом в деле защиты жертвы является принцип «не навреди» и необходимость действовать в наилучших интересах уязвимых субъектов данных.

5.3 Документирование публикации данных

Оператор данных обеспечивает регистрацию публикаций и ее сохранение.

Регистрационные записи о публикации данных включают все следующие пункты:

- дату публикации;
- если целесообразно, дату, когда необходимо пересмотреть основания для публикации в соответствии с ОЭЗД;

- если нужно, дату, когда данные должны быть удалены из открытого доступа;
- описание категорий персональных данных, которые были опубликованы;
- по возможности, подробности используемой медиа поддержки.

5.4 Данные, которые должны быть опубликованы для ВСС

Данные, которые могут быть опубликованы, должны определяться для каждого конкретного контекста, и более конкретные указания могут даваться в отношении конкретных категорий субъектов данных. На основании ОЭЗД конкретные меры могут включать следующее:

- ограничение публикации данными абсолютно необходимыми для того, чтобы дать возможность читающему/ слушающему определить лиц, чьи имена/ фотографии опубликованы, и восстановить связь;
- фотографии уязвимых лиц не должны опубликовываться вместе с другими персональными данными (например, именем), адреса несовершеннолетних лиц никогда не публикуются.

5.5 Данные, публикующиеся для государственных архивов

Персональные данные, которые были заархивированы, могут стать открытыми в соответствии с применимым законодательством.

5.6 Данные, публикующиеся для информирования общественности

В соответствии с применимым законодательством персональные данные могут опубликовываться для целей распространения информации о деятельности по ВСС и (или) привлечения внимания к ситуациям, вызывающим обеспокоенность. Информирование общественности связано также со свободой на получение информации и свободой слова, а также с подотчетностью. Однако, как и в случае с публикацией, принципы, изложенные в настоящем КП должны соблюдаться, а ОЭЗД проводиться.

5.7 Право отозвать согласие/ добиться уничтожения опубликованных материалов

Если опубликование имеет место на основании согласия, то субъект данных в любой момент времени может отозвать согласие на публикацию материалов, способствующих его идентификации. В этом случае оператор данных предпринимает все разумно необходимые шаги, принимая во внимание трудности, присущие процессу уничтожения открытых документов (особенно онлайн), для того чтобы отозвать опубликованные материалы и (или) предотвратить их публикацию.

Если опубликование имеет место на основании ином, нежели согласие, применяется

процедура, описанная в разделе 3.4 «Возражение против обработки данных».

6. Применение КП

Группа по применению КП будет оказывать поддержку выполнению КП на глобальном уровне, содействуя постоянному обучению и развитию.

При условии соблюдения национального законодательства настоящий КП должен эффективно применяться всеми операторами данных следующим образом:

- КП должен найти отражение в политике по ВСС, руководящих принципах и программах;
- КП должен стать неотъемлемой частью управления персоналом по ВСС и его подготовки каждого оператора данных;
- должно быть назначено контактное лицо по защите данных для ВСС и сообщаться контактные данные;
- операторы данных должны участвовать в периодических рассмотрениях выполнения КП;
- они должны сотрудничать с группой по применению КП;
- должен осуществляться мониторинг, который ведет к самоконтролю, диалогу, рассмотрению на уровне равных, другим формам рассмотрения и осуществляется на добровольной основе для обеспечения непрерывного совершенствования и обучения в рамках организации.

Группа по применению КП пересматривает и обновляет настоящий КП по мере необходимости.

7. Справочные материалы

7.1 Юридические документы/ руководящие принципы

- Директива 95/46/ЕС Европейского парламента и Совета Европейского Союза от 24 октября 1995 года о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных от 24 октября 1995 г.
<http://www.consultant.ru/online/>
- Договор о функционировании Европейского Союза (ДФЕС) от 13 декабря 2007, статья 16, <http://eulaw.ru/treaties/tfeu> ;
- Европейская конвенция о защите прав человека и основных свобод от 4 ноября 1959 г., статья 8;
- Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, Страсбург, 28 января 1981 года, Бюллетень международных договоров. 2014. № 4.
- Международный пакт о гражданских и политических правах, Статья 17;
- Организация экономического сотрудничества и развития (ОЭСР), Руководящие

принципы по защите частной жизни и трансграничных потоков персональных данных, 1980 г. (обновлено в 2013 г.) oe.cd/privacy;

- Руководящие принципы регламентации компьютеризованных картотек, содержащих данные личного характера, принятые резолюцией Генеральной Ассамблеи 49/95 14 декабря 1990 г.;
- Устав Международного движения Красного Креста и Красного Полумесяца с поправками 2006 г.;
- Хартия Европейского Союза об основных правах, статьи 7 - 8;
<http://eulaw.ru/treaties/charter>
- OECD Guidelines for Consumer Protection in the Context of Electronic Commerce, 9 December 1999, www.oecd.org/sti/consumer/34023811.pdf ;
- APEC Privacy Framework, 2005, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx
- Резолюция 4 Совета делегатов Международного движения Красного Креста и Красного Полумесяца о принятии Стратегии о восстановлении семейных связей, Женева, 23-24 ноября 2007 г. (См. Стратегия восстановления семейных связей. Включает юридический справочный материал, Москва, МККК, 2010, с. 15);
- International Conference of Data Protection and Privacy Commissioners, Resolution on Privacy and International Humanitarian Action, Amsterdam, Netherlands, 2015,
<https://icdppc.org/document-archive/adopted-resolutions/>
- International Standard on the protection of personal data and privacy by the International Conference of Data Protection and Privacy Commissioners, 5 November 2009,
http://privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf;

7.2 Основные Руководства

- Восстановление семейных связей при стихийных бедствиях и катастрофах. Практическое руководство. Москва, МККК, 2012.;
- Оценка потребностей в области восстановления семейных связей. Руководство для национальных обществ и МККК. Москва, МККК, 2011;
- Работа с останками в период после бедствий и катастроф. Практическое руководство для сотрудников служб быстрого реагирования. МККК совместно с ВОЗ и Международной федерацией, Москва, 2010;
- Стратегия восстановления семейных связей. Включает юридический справочный

материал, Москва, МККК, 2010;

- INTERNATIONAL COMMITTEE OF THE RED CROSS (ICRC), *Guidelines on providing restoring family links services to persons separated as a result of migration: an Internal document for the International Red Cross and Red Crescent Movement*, Switzerland, ICRC, 2010, 59 p.

ПРИЛОЖЕНИЯ

Приложение 1: Деятельность по ВСС и связанная с ВСС деятельность

Деятельность по ВСС может быть разного типа в зависимости от ситуации и контекста:

- организация обмена семейными новостями;
- розыск отдельных лиц;
- регистрация отдельных лиц (детей и взрослых) и отслеживание их судьбы с целью предотвращения их исчезновения и с тем, чтобы дать возможность их семьям получать информацию;
- воссоединение семей и репатриация;
- сбор информации об умерших, управление ею и ее передача;
- передача официальных документов, таких как свидетельства о рождении, удостоверения личности или различные другие сертификаты, выдаваемые властями;
- выдача свидетельств о содержании под стражей отдельных лиц и документов, свидетельствующих о других ситуациях, которые привели к регистрации отдельных лиц;
- выдача проездных документов МККК;
- мониторинг интеграции тех, кто воссоединился с членами семьи;
- содействие и оказание поддержки созданию механизмов для выяснения участи и местонахождения лиц, о которых нет никакой информации;

См. также: <http://familylinks.icrc.org>

Деятельность, связанная с ВСС - другие услуги гуманитарного характера, связанные с деятельностью по ВСС и предоставляемые сотрудниками по ВСС:

- материальная, правовая, психологическая и психосоциальная поддержка семей лиц, пропавших без вести, и других лиц, пострадавших в результате вооруженного конфликта, других ситуаций насилия, бедствий, миграции и других гуманитарных кризисов;
- оказание поддержки соответствующим властям в деле обращения с человеческими останками и судебной идентификации;
- услуги по социальному обеспечению (направление в соответствующие службы);
- услуги по переселению и реинтеграции для уязвимых групп населения (направление в соответствующие службы поддержки реинтеграции);
- архивирование (индивидуальная/ семейная память; память человечества; административные потребности отдельных лиц, отчетность сторон, исторические,

статистические и медицинские исследования);

- информирование общественности с целью содействия ВСС и деятельности, связанной с ВСС.

Приложение 2: *Общественный интерес*

Примерами общественного интереса могут служить ситуации:

- когда речь идет о крупномасштабных кризисах, требующих незамедлительных действий, и невозможно осуществлять деятельность на основании согласия и точно установить, применимо ли законное основание жизненно важного интереса; примером может послужить ситуация, когда значительное число мигрантов должны быть спасены в море;
- когда деятельность по обработке данных является очень сложной и вовлекает различных внешних обработчиков и сложные технологии, что затрудняет для субъектов данных понимание в полной мере рисков и преимуществ действий по обработке данных и поэтому принятие обоснованного решения. Когда жизненно важные интересы субъекта данных или другого лица не могут быть определены (либо из-за отсутствия срочности, либо потому, что субъект данных разыскивается), обработка может осуществляться на основании мандата оператора данных, при условии, что проведена удовлетворительная ОЭЗД;
- распределения продуктов помощи, если не реально получить согласия всех возможных получателей помощи и если, как можно обоснованно предположить, жизнь и неприкосновенность субъекта данных или других лиц не находится под угрозой (в этом случае наиболее правильным основанием для обработки может быть «жизненно важный интерес»);
- когда обрабатываются персональные данные субъекта данных, содержащегося под стражей. Это может произойти, например, при обработке персональных данных, связанных с лицами, лишенными свободы в контексте вооруженного конфликта или другой ситуации насилия, когда МККК (или национальное общество) пока не смогло осуществить посещение субъекта данных, лишенного свободы, и получить его согласие и когда условия содержания в каком-либо конкретном случае могут опровергать предположение о применимости основания «жизненно важный интерес».

Приложение 3: Законный интерес

К примерам законного интереса относятся ситуации, когда:

- обработка необходима для эффективного выполнения мандата оператора данных в соответствии с основополагающими принципами (особенно нейтральности, независимости и беспристрастности) и его стандартными условиями работы;
- обработка данных осуществляется строго в той степени, которая необходима для целей обеспечения безопасности информационных систем и информации и безопасности услуг, которые предлагаются этими информационными системами, государственными властями, группами быстрого реагирования на нарушения компьютерной безопасности (группами CERT), группами реагирования на инциденты, связанные с нарушением информационной безопасности (ГРИКБ), провайдерами сетей электронной коммуникации и службами и провайдерами технологий и услуг безопасности. Это могло бы, например, включать предотвращение несанкционированного доступа к электронным коммуникационным сетям и распространения враждебного программного кода, а также нападений типа «отказ в обслуживании» и повреждений компьютерных сетей и электронных коммуникационных сетей;
- обработка персональных данных осуществляется в строго необходимой степени для целей предотвращения, доказательства и пресечения мошенничества или хищения;
- обработка персональных данных осуществляется для того, чтобы сделать персональные данные анонимными или присвоить им псевдоним;
- когда это необходимо для установления, осуществления или защиты правомерных требований, независимо от того, какая процедура имеет место – судебная, административная или любая внесудебная; прямой маркетинг и (или) информирование общественности.

Приложение 4: Безопасность данных

Персональные данные должны обрабатываться таким методом, который обеспечивает должную безопасность персональных данных, в том числе предотвращение несанкционированного доступа к этим данным и к оборудованию, применяемому для обработки, и их неправомерное использование.

Любое лицо, действующее под началом оператора данных и имеющее доступ к персональным данным, должно обрабатывать их исключительно способом, соответствующим КП и применимой политике безопасности данных, как разъясняется далее в настоящем Приложении.

Для обеспечения безопасности и предотвращения обработки в нарушение настоящего КП оператор данных оценивает конкретные риски, присущие процессу обработки, и принимает меры для их снижения. Эти меры должны обеспечить должный уровень безопасности (с учетом имеющейся технологии, сложившейся обстановки в области безопасности и условий логистики, а также стоимости имплементации), принимая во внимание риски и характер персональных данных, которые подлежат защите. Сюда относятся меры, включающие:

- подготовку;
- управление правами доступа к базам данных, содержащих персональные данные;
- физическую безопасность баз данных;
- информационную безопасность;
- положения о неразглашении;
- методы уничтожения персональных данных;
- любые другие соответствующие меры.

Цель этих мер заключается в том, чтобы обеспечить сохранность персональных данных, как с технической, так и организационной точек зрения, и их защиту посредством принятия разумных и соответствующих мер против несанкционированного изменения, копирования, манипуляций, незаконного уничтожения, случайной утраты, ненадлежащего раскрытия или неправомерной передачи.

Меры обеспечения безопасности данных могут быть различными в зависимости, среди прочего, от:

- типа операций;
 - характера и конфиденциальности персональных данных;
 - формы или формата хранения;
 - окружения/ местоположения конкретных персональных данных; и
 - сложившихся условий безопасности и логистики.
-

Меры обеспечения безопасности данных должны регулярно пересматриваться и обновляться для обеспечения того уровня защиты, который соответствует степени секретности, применимой к персональным данным.

Оператор данных отвечает за координацию действий в перечисленных ниже областях.

- Создание системы управления информационной безопасностью. Для этого он разрабатывает и регулярно обновляет Политику безопасности данных, основанную на международно-признанных стандартах и на оценке рисков. Она должна состоять, например, из Руководящих принципов обеспечения физической безопасности, Политики информационной безопасности, Руководства по безопасности электронной почты, Руководства по использованию компьютерного оборудования, Типологии обработки информации, Плана на случай чрезвычайных обстоятельств и Принципов уничтожения документов.
- Разработка коммуникационной инфраструктуры и баз данных для того, чтобы сохранить неприкосновенность и безопасность данных в соответствии с принятой политикой обеспечения безопасности.
- Принятие в соответствии с настоящим КП всех соответствующих мер по защите безопасности обрабатываемых данных в информационной системе оператора данных.

1. Права доступа к базам данных

Оператор данных отвечает за:

- предоставления доступа к базам данных, содержащих персональные данные;
- безопасность оборудования, которое дает возможность уполномоченному персоналу иметь доступ к этой системе;
- соблюдение правил безопасности, указанных в настоящем Приложении;
- обеспечение того, что получившие доступ сотрудники в состоянии соблюдать настоящий КП. Это включает подготовку, обязательство о неразглашении, предусматриваемое в подписанном договоре о найме до предоставления права доступа к базам данных;
- предоставление доступа только на основании принципа «необходимо знать»;
- ведение реестра сотрудников, имеющих доступ к каждой базе данных и обновление его по необходимости (например, сотрудники могут получить другие обязанности, не связанные более с необходимостью доступа к данным);
- если это практически возможно, ведение для обеспечения отчетности журнала регистрации всех сотрудников, которые имели доступ к базе данных, в течение всего срока, когда данные, обработанные такими сотрудниками, находятся в базе данных

Сотрудники обрабатывают данные в пределах предоставленных им прав на обработку данных.

Сотрудники, имеющие более высокий уровень права доступа или отвечающие за управление правами доступа, могут иметь дополнительные договорные обязательства,

касающиеся неразглашения информации.

2. Физическая безопасность

Каждый оператор данных несет ответственность за:

- формулирование правил безопасности, определяющих процедурные, технические и административные средства обеспечения безопасности, которые должны гарантировать соответствующий уровень конфиденциальности, а также физическую неприкосновенность и доступность баз данных (как физических, так и компьютерных) учетом выявленных рисков;
- обеспечение того, что персонал информирован о таких правилах безопасности и соблюдает их;
- разработку соответствующих механизмов контроля для обеспечения поддержания безопасности данных;
- обеспечение применения адекватных электротехнических и противопожарных стандартов в местах хранения;
- обеспечение того, что объемы хранения строго соответствуют необходимому минимуму.

3. Информационная безопасность

Оператор данных должен:

- сформулировать правила безопасности, определяющие процедурные, технические и административные средства обеспечения безопасности, гарантирующие соответствующий уровень конфиденциальности, а также неприкосновенность и доступность используемых информационных систем на основании оценки рисков;
- разработать соответствующие механизмы контроля для обеспечения безопасности данных;
- установить конкретные правила безопасности для части IT инфраструктуры, базы данных или особого отдела, если сочтет это необходимым.

Вся корреспонденция, как внешняя, так и внутренняя, ведущаяся по электронной почте и содержащая персональные данные, обрабатывается на основании принципа "необходимо знать". Получатели корреспонденции по электронной почте тщательно отбираются, чтобы избежать ненужного распространения персональных данных.

Удаленный доступ к серверам и использование своих настольных ПК, или портативных компьютеров, должны соответствовать стандартам безопасности, указанным в Политике информационной безопасности оператора данных. Если это не является абсолютно необходимым в силу оперативных причин, следует избегать использования Интернета и незащищенных беспроводных соединений для того, чтобы извлечь персональные данные, обменяться ими или передать их.

Персонал, работающий с персональными данными, с должным вниманием и

осторожностью подключается к удаленным серверам оператора данных. Пароли должны постоянно защищаться, и сотрудники должны проверять, что они должным образом выходят из компьютерных систем, а открытые браузеры отключены.

Ноутбуки, смартфоны и другое портативное оборудование требует особых мер предосторожности, особенно при работе в трудных условиях. Портативное коммуникационное оборудование должно всегда храниться в местах, где обеспечена его безопасность и сохранность.

Портативные или передвижные устройства не должны использоваться для хранения документов, содержащих персональные данные, которые классифицируются как особенно конфиденциальные. Если этого нельзя избежать, персональные данные должны пересылаться в соответствующие компьютерные системы и приложения баз данных как можно скорее. Если флэш-память, например, USB флеш-накопители и карты памяти используются для временного хранения персональных данных, она должна храниться в безопасности и электронные записи должны быть зашифрованы. Информация должна удаляться с портативных или передвижных устройств после того, как она запоминается должным образом, если больше не требуется такой поддержки.

Восстановление и резервная копия

Эффективные механизмы восстановления и процедуры создания резервных копий должны применяться ко всем электронным записям, а соответствующий сотрудник, отвечающий за информационную и коммуникационную систему (ИКТ) должен обеспечить регулярно выполняемые процедуры создания резервных копий. Частотность этих процедур будет разной в зависимости от конфиденциальности персональных данных. Электронные записи должны быть автоматизированы, что позволит легкое восстановление в ситуациях, когда процедуры создания резервных копий затруднены, *inter alia*, из-за частых отключений питания, системных сбоев или стихийных бедствий.

Когда электронные записи и приложения базы данных более не нужны, оператор данных должен скоординировать действия с соответствующим сотрудником по ИКТ (ИКТ) для обеспечения постоянного удаления.

4. Обязательство о конфиденциальности и поведение персонала

Обязательство о соблюдении принципа конфиденциальности является ключевым элементом безопасности персональных данных. Это обязательство заключается в том, что:

- все сотрудники и внешние консультанты подписывают соглашение о неразглашении и конфиденциальности, что является частью их договора о найме или о предоставлении консультационных услуг; это требование выдвигается наряду с требованием того, что персонал должен обрабатывать данные только в соответствии
-

с указаниями оператора данных;

- любой внешний обработчик данных обязан соблюдать положения о конфиденциальности в соответствии с контрактом; это требование выдвигается наряду с требованием о том, что обработчик должен обрабатывать данные только в соответствии с указаниями оператора данных;
- должна строго применяться Типология обработки информации, основанная на ее статусе конфиденциальности; и
- любая просьба субъектов данных о том, что их персональные данные должны обрабатываться определенным образом и, в частности, что они должны считаться конфиденциальными и не передаваться третьим сторонам, должна гарантированно аккуратно регистрироваться в файле субъекта данных.

Для того чтобы снизить опасность утечки, только уполномоченный персонал отвечает за сбор и управление данными из конфиденциальных источников и имеет доступ к документам в соответствии с применимой Типологией обработки информации;

Сотрудники отвечают за присвоение уровня конфиденциальности данным, которые они обрабатывают, на основании применимой Типологии обработки информации и за соблюдение конфиденциальности данных, к которым они обращаются за справкой и которые они передают или используют для целей внешней обработки.

Сотрудники, которые изначально присвоили данным уровень конфиденциальности, могут в любое время изменить его, в частности, присвоив более низкий уровень конфиденциальности, чем ранее указанный, если они считают, что данные требуют меньше защиты.

5. Планирование на случай чрезвычайных обстоятельств

Оператор данных отвечает за разработку и выполнение плана эвакуации записей в случае чрезвычайных обстоятельств.

6. Методы уничтожения

Когда определено, что сохранение персональных данных более не является необходимым, все записи и резервные копии должны быть уничтожены или сделаны анонимными.

Метода уничтожения будет зависеть, *inter alia*, от:

- характера и уровня конфиденциальности персональных данных;
- формата и носителя информации; и
- объема электронных записей и записей на бумажных носителях.

Оператор данных проводит оценку конфиденциальности до уничтожения для того, чтобы

обеспечить использование соответствующего метода уничтожения персональных данных.

Уничтожение записей на бумажном носителе

Записи на бумажном носителе уничтожаются таким методом, как измельчение или сжигание, что не даст возможности использовать или восстановить их в будущем.

Если принято решение, что записи на бумаге следует перевести в цифровые записи, то после тщательного переноса записей в электронный формат все следы записей на бумажном носителе следует уничтожить, если только сохранение бумажных носителей не требуется применимым национальным правом или если бумажная копия не должна сохраняться для целей архивирования.

Уничтожение электронных записей

Уничтожение электронных записей должно поручаться соответствующему ICT персоналу, поскольку функция стирания в компьютерных системах не обязательно обеспечивает полное уничтожение.

Получив инструкции соответствующий ICT персонал должен обеспечить полное удаление всех следов персональных данных из систем компьютера и другого программного обеспечения.

Дисковые накопители и приложения баз данных должны быть стерты, и все перезаписываемые средства, такие как, среди прочего, CD, DVD, микрокарты, видео- и аудио ленты, которые используются для хранения персональных данных, должны быть очищены перед повторным использованием. Физические меры уничтожения электронных записей, такие как утилизация, измельчение или сжигание, должны применяться при строгом мониторинге.

Регистрация уничтожения

Оператор данных должен обеспечить включение во все соответствующие договоры об оказании услуг, МОВ, соглашения и письменные контракты о передаче или обработке период сохранности записи, предусматривающий уничтожение персональных данных после выполнения конкретной задачи. Третьи стороны должны вернуть персональные данные оператору данных и подтвердить, что все копии персональных данных были уничтожены, включая персональные данные, предоставленные их уполномоченным агентам и субподрядчикам. Регистрационные записи об уничтожении, в которых указывается время и метод уничтожения, а также характер уничтоженных записей, должны сохраняться и прилагаться к докладам о проекте или оценке.

Уничтожение больших объемов записей на бумажных носителях может быть поручено специализирующимся в этом компаниям. В таких обстоятельствах оператор данных должен обеспечить соблюдение конфиденциальности персональных данных, подтвержденное в письменной форме, и включение условия о представлении записей об уничтожении и сертификатов уничтожения в качестве части договорных обязательств третьих сторон.

7. Другие меры

Безопасность данных требует также наличия соответствующих внутренних организационных правил, включающих регулярное информирование всех сотрудников о правилах безопасности данных и об их обязанностях в соответствии с законом о защите данных, особенно обязанностей, касающихся конфиденциальности

Назначение сотрудника, отвечающего за безопасность

Каждый оператор данных поручает выполнение функций должностного лица, отвечающего за безопасность, одному или нескольким штатным сотрудникам (возможно, администратору или IT специалисту), которые будут выполнять операции по обеспечению безопасности.

Сотрудник, отвечающий за безопасность, в частности:

- обеспечивает выполнение процедур, гарантирующих безопасность и указанных в настоящем КП и в действующих правилах безопасности;
 - обновляет эти процедуры по мере необходимости;
 - проводит подготовку персонала по вопросу о безопасности данных.
-

Приложение 5: Информация, которая должна быть предоставлена

Предоставляемая информация	Согласие	Жизненно важный интерес/ общественный интерес	Законный интерес	Договорное/ юридическое обязательство
Оператор данных /ответственные сотрудники	да	да	да	да
Цель обработки	да	да	да	да
Предполагаемые внешние обработчики	да	ОЭЗД и раскрытие информации личного характера, если возможно	да	да
Планируемые передачи	да	ОЭЗД и раскрытие информации личного характера, если возможно	да	да
Права субъекта данных (информация, доступ, исправления, уничтожение, возражение)	да	ОЭЗД и раскрытие информации личного характера, если возможно	да	да
Если применимо, предоставляются ли данные на основании права/ договора	Не применимо	Не применимо	да	да

Приложение 6: Краткое руководство по ОЭЗД

Цель оценки эффективности защиты данных (ОЭЗД) заключается в том, чтобы выявить и оценить особые риски для персональных данных, возникающие в результате некоторых видов деятельности по восстановлению семейных связей (ВСС), и найти решение возникающих в связи с этим проблем. ОЭЗД должна привести к принятию мер, направленных на устранение, минимизацию или смягчение этих рисков. Цель настоящего руководства по ОЭЗД заключается в том, чтобы дать возможность сотрудникам сети ВСС провести ОЭЗД. **Схема ОЭЗД для деятельности по ВСС**, предлагая примеры видов рисков и возможных мер по их смягчению, **может быть предоставлена национальным обществам в виде отдельного документа.**

Вот некоторые ситуации, когда следует рассмотреть возможность провести ОЭЗД.

- Ваша организация хранит свои файлы на дисках и на бумаге. Теперь вы хотите ввести централизованное электронное хранение файлов. Как решить, где лучше всего хранить какую информацию?
- Цунами сметает с лица земли десятки прибрежных деревень. Тысячи людей считаются пропавшими без вести. Какой объем информации личного характера вы должны собрать у семей лиц, пропавших без вести? Нужно много информации или ее минимум? Должна ли она включать конфиденциальную информацию (например, ДНК, религию, политические предпочтения)?
- Правительство создает систему для централизации всей информации о лицах, пропавших без вести в результате цунами. Оно просит вас предоставить всю информацию, которой вы располагаете, о лицах, пропавших без вести в результате этого события. Какой объем информации личного характера следует ему сообщить для розыска пропавших людей? На каких условиях следует сообщать ему информацию личного характера?
- Другая гуманитарная организация просит вас сообщить данные о людях, проживающих в лагере для беженцев. Должны ли вы сообщать такую информацию? На каких условиях? Каковы последствия сообщения такой информации? Будет ли организация столь же осмотрительна по отношению к персональным данным, как и вы?
- Можете ли вы опубликовать фотографии безнадзорных детей, разыскивающих своих родственников через Интернет? Можно ли сделать плакаты с фотографиями детей, пропавших без вести? На каких условиях и при каких обстоятельствах?
- Одна социальная сеть предлагает помочь вам в деле восстановления семейных связей после бедствия. Каким образом вы можете сотрудничать с этой социальной сетью, не нанося ущерба безопасности персональных данных и лиц, которых это касается?
- Завтра МККК планирует посещение места содержания под стражей, где, как сообщается, находится разыскиваемое лицо. Принимая во внимание срочность дела, можете ли вы передать в МККК запрос о розыске или послание Красного Креста по электронной почте?

В некоторых обстоятельствах может не быть достаточного времени для проведения ОЭЗД в полном объеме, либо сложность, конфиденциальность и масштаб операции по обработке не требует официальной ОЭЗД. Тем не менее, сотрудники сети ВСС должны при принятии решений о передаче данных всегда помнить об оценке риска в отношении защиты данных. Поэтому персонал ВСС и добровольцы должны понимать процесс ОЭЗД и рассмотреть вопрос, поставленный ниже.

Процесс ОЭЗД обычно состоит из следующих этапов. Эти этапы должны найти отражение в докладе о ОЭЗД:

A. Определение круга задач

1. Основываясь на информации о сложности, конфиденциальности и масштабах операции по обработке, определите:

- является ли ОЭЗД необходимой;
- кто будет проводить ОЭЗД;
- кто будет осуществлять контроль и утверждать процедуру ОЭЗД.

2. В контексте деятельности по ВСС опишите, как персональные данные собираются, используются, хранятся и передаются. Это включает составление схемы заинтересованных сторон и описание потоков информации (т.е., какая информация собирается, у кого, кем; как эта информация используется; как, где и как долго хранится; используются ли услуги внешних обработчиков, кто имеет доступ к информации?).

3. Определите заинтересованные стороны, с которыми можно проконсультироваться. Это могут быть ваши сотрудники (например, IT специалист, юридический советник, психолог, специалисты программы...) или внешние заинтересованные стороны (такие как другие организации, правительственные учреждения, социальные работники, общинные руководители, законные опекуны...).

B. Оценка

4. Определите риски для отдельных лиц, возникающие в результате операции по обработке и риски несоблюдения Кодекса поведения в области защиты данных.

5. Оцените риски.

6. Определите меры для устранения, минимизации или снижения уровня рисков.

7. Предложите рекомендации.

C. Одобрение и выполнение

8. Обратитесь с просьбой о проведении проверки и получите одобрение.

9. Выполните согласованные рекомендации.

10. Внесите изменения в ОЭЗД, если изменения имеют место и в деятельности.

Если ОЭЗД проводится, это должно найти отражение в докладе (содержащем информацию о А), В) и С) выше). В зависимости от сложности, конфиденциальности и масштабов операций по обработке **доклад** по ОЭЗД (результат процесса ОЭЗД) может быть очень коротким или более тщательным и подробным. Доклад по ОЭЗД может включать модель, предоставляемую отдельно каждому национальному обществу.

Приложение 7: Выполнение юридического обязательства

Может включать, в зависимости от обстоятельств оператора данных:

- соблюдение национального или регионального права, например, в области трудового законодательства, финансовой отчетности, мошенничества, отмывания денег;
 - распоряжения суда.
-