Сеть по воссоединению семейных связей
Кодекс поведения в отношении защиты данных
Схема оценки эффективности защиты данных (ОЭЗД)

До проведения ОЭЗД национальным обществам следует рассмотреть следующие вопросы:

- Имели ли место консультации с заинтересованными сторонами в рамках Движения относительно рисков, возникающих в результате операций по обработке, и рисков, связанных с несоблюдением Кодекса поведения?
- Были ли проведены консультации с внешними заинтересованными сторонами?
- Кроме вопроса определения рисков, обсуждались ли во время консультаций меры по предотвращению или минимизации рисков?

| **Вопрос, связанный с защитой данных** | **Кодекс поведения** | **Оценка рисков** | **Меры по снижению риска** | **Вывод** |
|---|---|---|---|---|
| <u>Определение цели</u><br><br>Будут ли данные, которые предстоит собрать, использоваться только для указанной цели?<br><br>Будут ли собранные данные использованы для иной цели, нежели указанная? | 2.1 Точно определенная цель | **Пример**: “расширение сферы использования” – национальные общества могут захотеть получить больше пользы от данных, которые они собирают.<br><br>**На практике:** национальные общества могут пренебречь требованием не использовать персональные данные в других целях или не знать о нем (т.е. использовать данные, которые они изначально собрали, для каких-то дополнительных целей) и не получить на это дополнительного согласия.<br><br>➢ Национальное общество может не соблюдать Кодекс поведения в области ВСС | **Примеры:**<br>▪ Укажите точно/задокументируйте цели, для которых будут собираться/ использоваться персональные данные<br>▪ Привлеките внимание к Кодексу поведения в области ВСС, который предусматривает принцип точного определения цели и дельнейшую обработку только для целей, соответствующих первоначально указанной цели сбора данных.<br>▪ Улучшите подготовку персонала в отношении определения цели/ соответствующей дальнейшей обработки.<br>▪ Использование базы данных: в качестве части подхода, основанного на принципе неприкосновенности частной жизни, включите в файл указание, обеспечивающее обязательное разъяснение цели обработки данных. Если целесообразно, свяжите цель | Уровень риска достаточно снижен<br><br>Уровень риска не обязательно снижен, но риск принимается<br><br>Уровень риска не снижен, риск не принимается |

| Вопрос, связанный с защитой данных | Кодекс поведения | Оценка рисков | Меры по снижению риска | Вывод |
|---|---|---|---|---|
| | | | операций по обработке данных с согласием, которое могло быть дано. | |
| <u>Ограничения</u><br>Нужны ли все собранные персональные данные для деятельности по ВСС?<br><br>Когда люди сотрудничают с вами, надеясь получить помощь, сообщают ли им, как информация личного характера, которую они предоставляют, будет использоваться? | 2.3.2 Обработка адекватных, относящихся к делу и обновленных данных.<br><br>2.3.1 Ответственность и подотчетность<br><br>2.2.1 Согласие<br>3.1 Информация и доступ | **Пример:** национальное общество может собрать больше персональных данных, чем это необходимо для указанной цели<br><br>**На практике**: Репутации национального общества может быть нанесен ущерб, если станет известно, что его сотрудники собирают больше персональных данных, чем это действительно нужно.<br><br>➢ Собранные избыточные персональные данные становятся причиной более высокого уровня риска для получателей помощи/ их семей/ свидетелей/ или других лиц, если незаконно получен доступ к системе либо она иным образом подвергается риску (несанкционированное использование/ разглашение или нарушение правил безопасности).<br><br>➢ Сбор большего объема данных, чем необходимо, также может повысить риск хищения | **Примеры:**<br>▪ Гарантируйте, что ваши сотрудники собирают только те данные, которые необходимы для достижения изначально указанной цели.<br>▪ Если возможно, заранее ознакомьте людей с условиями/ целями сбора данных и их обработки. Дайте людям возможность задать вопросы о способе сбора и обработки данных и цели, для которой собираются и обрабатываются их персональные данные. | Уровень риска достаточно снижен<br><br>Уровень риска не обязательно снижен, но риск принимается<br><br>Уровень риска не снижен, риск не принимается |

| Вопрос, связанный с защитой данных | Кодекс поведения | Оценка рисков | Меры по снижению риска | Вывод |
|---|---|---|---|---|
| | | информации, удостоверяющей личность, в том числе для совершения мошенничества. | | |
| <u>Право на информацию</u><br><br>Сообщается ли лицам в явной форме о том, почему собираются их персональные данные и как они могут использоваться? | 3.1 Информация и доступ | **Пример**: национальные общества не предоставляют людям четкой и легко доступной информации относительно своей политики, процедур и практики в области сбора информации<br><br>**На практике:** какой-то человека хотел бы отыскать своего родственника, но опасается делать это, поскольку не совсем понимает процедуры обработки/ передачи данных, которые применяются национальным обществом.<br><br>➢ Если стандарты и процедуры сбора и обработки данных не являются прозрачными, люди могут не доверять им и не предоставлять свои персональные данные.<br>➢ Национальное общество может не действовать в соответствии с Кодексом поведения в области ВСС | **Примеры**:<br>▪ Если бы у национального общества была специальная Web-страница, там могла бы быть закладка, связывающая лицо с Кодексом поведения в области ВСС.<br>▪ Национальные общества могли бы также разработать документ «Вопросы и ответы», где суммировались бы положения КП в области ВСС, и распечатать на бумаге копии для субъектов данных<br>▪ Кроме того, следует создать ссылку на сайте «Семейные связи» или на национальных сайтах, где будет рассказано о характере деятельности в целом, а также об общих условиях сбора и обработки данных. | Уровень риска достаточно снижен<br><br>Уровень риска не обязательно снижен, но риск принимается<br><br>Уровень риска не снижен, риск не принимается |
| <u>Правовые основания для обработки/ передачи данных</u> | 2.1 Точное определение | Пример:<br>▪ Один или несколько | **Пример:**<br>▪ Рассмотрите процесс, | Уровень риска достаточно снижен |

| Вопрос, связанный с защитой данных | Кодекс поведения | Оценка рисков | Меры по снижению риска | Вывод |
|---|---|---|---|---|
| <u>Согласие</u><br>Могут ли люди оценить наиболее вероятные последствия (включая отрицательные)? Связана ли обработка данных со сложными технологическими процессами? Свободен ли действительно выбор человека относительно дачи своего согласия?<br><br>Могут ли люди отказаться от предоставления некоторых или всех данных и не быть за это наказанными каким-либо образом или не лишиться помощи, которую ваша организация могла бы иначе предоставить?<br><br>Как люди дают согласие на то, чтобы их данные собирались? Если согласие дано не в письменной форме, не видите ли вы в этом какую-либо опасность?<br><br>Ограничивается ли согласие конкретно указанной целью? Если персональные данные предстоит использовать для цели иной, нежели изначально указанная (вторичная цель), нужно ли получать новое согласие соответствующего лица?<br><br>Согласился ли человек явным образом на то,<br>как его данные могут использоваться или на то, что они могут передаваться другим организациям?<br><br>Существуют ли примеры или обстоятельства, когда лицо дало согласие на передачу или разглашение | цели<br><br>2.2 Законная и справедливая обработка данных<br><br>2.2.1 Согласие<br><br>3.1 Информация и доступ | человек угрожают публично заявить о том, что они не давали согласия на сбор национальным обществом их персональных данных.<br>▪ Правозащитная организация может обнаружить примеры того, когда национальное общество не получило согласие какого-либо лица.<br>▪ Мошенник из числа сотрудников распространяет информацию о том, что национальное общество не добивается получения обоснованного согласия.<br><br>**На практике:**<br>▪ Национальное общество обычно не получает от лиц подписанной формы, свидетельствующей об их согласии на сбор и использование их персональных данных<br><br>➢ Плохо для репутации национального общества.<br>➢ Другие возможные информанты решают, что неосмотрительно или небезопасно разговаривать с | посредством которого получается согласие. Разъясните бенефициариям или их семьям, свидетелям или другим соответствующим третьим сторонам, каковы могут быть последствия регистрации в национальном обществе, как их данные могут быть использованы в базе данных и кому они могут быть переданы в дальнейшем.<br>▪ Постарайтесь, если возможно, получить подписанное письменное обоснованное согласие.<br>▪ Было бы хорошо иметь на Web-странице национального общества закладку, разъясняющую, что такое обоснованное согласие.<br>▪ Обеспечьте логичность и доступность формы (бланка) согласия, включая печатную копию/ формы онлайн для применения всех методов сбора информации, в том числе по телефону.<br>▪ Обеспечьте доступность формы(бланка) согласия на всех соответствующих языках для целевой группы | Уровень риска не обязательно снижен, но риск принимается<br><br>Уровень риска не снижен и риск не принимается |

| Вопрос, связанный с защитой данных | Кодекс поведения | Оценка рисков | Меры по снижению риска | Вывод |
|---|---|---|---|---|
| информации личного характера, но сотрудники, отвечающие за это, считают, что делать этого не следует?<br><br><u>Альтернативные правовые основания</u><br><br>Собираются ли данные также и о лицах, которые отсутствуют? | | национальным обществом. | ▪ Если невозможно получить обоснованное согласие: обрабатывайте/ передавайте персональные данные, опираясь на альтернативные правовые основания (жизненно важные интересы, общественные интересы, законные интересы, выполнение юридического обязательства) | |
| | | | | |
| <u>Право доступа /Исправление / Уничтожение</u><br><br>Предоставляется ли лицам возможность получить доступ к их персональным данным и внести в них исправления?<br><br>Могут ли они обратиться с просьбой уничтожить некоторые или все свои персональные данные?<br><br>Необходимо ли ограничивать доступ к | 3.1 Информация и доступ<br><br>3.3 Исправление и уничтожение | **Пример:** Некоторые лица могут пожаловаться на то, что трудно увидеть и, если нужно, исправить (или даже уничтожить) их персональные данные<br><br>**На практике:** У национального общества может не существовать конкретных/ прозрачных процедур предоставления субъектам данных доступа к | **Примеры:**<br>▪ Если бы у национальных обществ были посвященные этому вопросу Web-страницы, на них могла бы быть закладка, по которой можно получить заверения в том, что национальное общество поможет людям в удовлетворении их просьб о доступе к их данным.<br>▪ Web-страница могла бы также давать точную информацию об условиях доступа (без ущерба | Уровень риска достаточно снижен<br><br>Уровень риска не обязательно снижен, но риск принимается<br><br>Уровень риска не снижен и риск не принимается. |

| Вопрос, связанный с защитой данных | Кодекс поведения | Оценка рисков | Меры по снижению риска | Вывод |
|---|---|---|---|---|
| данным? Если «да», то адекватно ли эти ограничения обусловлены и разъяснены? | | их персональным данным.<br><br>➢ Плохо для репутации<br>➢ О жалобах отдельных лиц может стать известно СМИ или правозащитным организациям. | для принципа конфиденциальности, который может применяться к определенным данным). | |
| <u>Качество и точность информации</u><br><br>Какие существуют процессы для обеспечения качества информации, т.е. того, что информация имеет отношение к делу, является надежной, точной и дающей основание для предъявления иска (и имеет значение для применения на практике)?<br><br>Существует ли политика или процедура для исправления данных, которые уже были переданы партнерам, или для уведомления партнеров о внесении обновлений? | 2.3.2 Обработка адекватных, относящихся к делу и обновленных данных<br><br>3.3 Исправления и уничтожение<br><br>3.4 Возражение | **Пример:**<br>▪ Сотрудники национальных обществ не располагают достаточным временем для того, чтобы проверить надежность информации, которую они получают от бенефициариев, их семей или свидетелей.<br>▪ Никто не является или очень немногие являются свидетелями события или только видят, как кого-то увозят, но не знают, что с ними случилось. Сотрудники национального общества вынуждены полагаться на неполную информацию или не могут ее проверить. У сотрудников недостаточно ресурсов для проверки заявлений.<br>▪ Некоторые сотрудники считают, что людям следует оказать помощь, даже если нет возможности проверить их жалобы и заявления. | **Примеры:**<br>▪ Обеспечьте до регистрации данных наличие процесса контроля качества для того, чтобы свести к минимуму ошибки или несанкционированные изменения.<br>▪ Если возможно, перепроверьте информацию, полученную от кого-либо, у других организаций, которые также могли опросить этого человека или других свидетелей.<br>▪ Разработайте процедуры для определения того, когда и как часто информация личного характера должна пересматриваться и (или) обновляться и когда данные должны уничтожаться или архивироваться.<br>▪ Разработайте процедуру для уведомления получателей данных о последующих исправлениях.<br>▪ Проводите различие между первичными и вторичными источниками данных и отразите эту разницу в файле посредством оговорки. | Уровень риска достаточно снижен<br><br>Уровень риска не обязательно снижен, но риск принимается<br><br>Уровень риска не снижен и риск не принимается |

| Вопрос, связанный с защитой данных | Кодекс поведения | Оценка рисков | Меры по снижению риска | Вывод |
|---|---|---|---|---|
| | | **На практике:** перенос записей с бумажного носителя в цифровой формат или в онлайн методом транскрибирования данных увеличивает риск внесения неточностей.<br><br>➢ Национальные общества могут принимать решения, основываясь на неполных, ненадежных или неправильных данных.<br>➢ Плохое качество информации может привести к неправильным решениям, что будет иметь отрицательные последствия для соответствующих лиц. | | |
| <u>Соответствующие меры безопасности</u><br><br>Какую персональную информацию следует собирать? Может ли разглашение этой информации подвергнуть лицо опасности (например, информация об этнической принадлежности, религии, сексуальной ориентации, политических взглядах, членстве в профессиональном союзе и т.п.).<br>Существует ли опасность того, что информация будет украдена/ утрачена/ изменена, что она станет недоступной, | 2.3.7 Безопасность<br><br>2.3.8 Компрометация данных<br><br>2.3.1 Ответственность и подотчетность<br><br>6. Применение Кодекса поведения | **Пример:**<br>▪ Внешние хакеры и мошенники из числа сотрудников могут попытаться воспользоваться персональными данными.<br>▪ Правительство может захотеть узнать данные всех лиц, которым МККК оказывает помощь.<br>▪ В ситуации насилия офисы национальных обществ могут | **Примеры:**<br>▪ Предупреждайте сотрудников о том, что следует избегать использования не имеющих защиты портативных устройств, таких как карты памяти.<br>▪ Разработайте надёжные протоколы контроля, которые ограничивают доступ на основании принципа служебной необходимости. Пользователи должны иметь доступ только к той части данных, которые им нужны для выполнения их | Уровень риска достаточно снижен<br>Уровень риска не обязательно снижен, но риск принимается<br><br>Уровень риска не снижен, и риск не принимается |

| Вопрос, связанный с защитой данных | Кодекс поведения | Оценка рисков | Меры по снижению риска | Вывод |
|---|---|---|---|---|
| что система подвергнется атаке хакеров или за организацией будет установлен контроль? Какие существуют действующие превентивные меры?<br><br>Вовлечены ли внешние организации или третьи стороны в обработку данных? Не увеличивает ли это опасность слежки/ разглашения обработчиком (как законное, так и нет)/ несанкционированной попытки доступа / краже данных/ доступности?<br><br>Ограничен ли доступ к информации на основании принципа служебной необходимости? Как это осуществляется на практике?<br><br>Напоминается ли сотрудникам держать файлы на бумаге, CD и (или) картах памяти запертыми или при себе всегда, когда они не используются? Поощряется ли персонал к зашифровке карт памяти?<br><br>Проводится ли для всех сотрудников подготовка по методам соответствующей защиты данных и обеспечения безопасности информации?<br><br>Шифруются ли сообщения по электронной почте? Какой тип кодирования используется?<br><br>Какие шаги будут предприняты, если будет иметь место нарушение правил | | обыскиваться и подвергаться грабежу.<br><br>**На практике:**<br>▪ Национальное общество может не научить сотрудников придерживаться практики, обеспечивающей безопасность информации.<br>▪ Оно может не ввести строгого контроля над доступом к его базе данных.<br>▪ Сотрудники могут пользоваться легко раскрываемыми паролями и могут не зашифровывать данные.<br>▪ Некоторые данные (например, блокноты) на бумажных носителях не дублируются и могут находиться только в офисах.<br><br>➢ Контроль за безопасностью системы национального общества нарушен, и персональные данные находятся в опасности.<br>➢ Национальное общество не знает, когда хранящиеся у него персональные данные | законный функций.<br>▪ Обеспечьте четкость и ясность в отношении того, кто имеет полномочия разрешать и отзывать разрешения на доступ или изменять его условия.<br>▪ Обеспечьте внесение в журнал регистрации операций по обработке всех случаев доступа к базе данных.<br>▪ Введите процедуры информирования субъектов данных о нарушениях правил обеспечения безопасности данных. | |

| Вопрос, связанный с защитой данных | Кодекс поведения | Оценка рисков | Меры по снижению риска | Вывод |
|---|---|---|---|---|
| безопасности данных? Информируются ли субъекты данных, если их персональные данные утрачены, украдены или иным образом подверглись риску? Будет ли информирована об этом какая-либо другая организация?<br><br>Рассмотрели вы некоторые из наихудших сценариев, касающихся того, что может случиться, если персональные данные, собранные вашей организацией, подвергнутся разглашению или опасности либо будут уничтожены случайно или преднамеренно?<br><br>Как вы будете решать, какие риски наиболее вероятны и какие, скорее всего, будут иметь наиболее сильное воздействие, если персональные данные будут украдены, подвергнутся хакерской атаке или изменены? | | оказываются в опасности.<br><br>➢ Наносится ущерб его репутации.<br>➢ Компрометация данных подвергает опасности жизнь людей. | | |
| <u>Сообщение информации, ее разглашение/ публикация и (или) передача</u><br><br>Будут ли персональные данные сообщаться другим организациям, включая национальные общества? Почему?<br><br>Предоставили ли они в письменном виде гарантии того, что они будут хранить информацию и не поделятся с ней больше ни с кем? Есть ли у организации адекватная политика | 4. Передача данных<br><br>2.3.1 Ответственность и подотчетность<br><br>1.4.3 Конфиденциальность<br><br>2.3.2 Обработка адекватных, относящихся к | **Пример:** Сотрудники могут сообщить персональные данные другим организациям или органам власти, но не могут контролировать, как эти другие организации или органы власти используют эти данные и не передают ли их дальше.<br><br>**На практике:** публикация фотографий безнадзорных детей может привлечь внимание торговцев детьми. | **Примеры:**<br>▪ Сообщайте информацию личного характера другим организациям или органам власти, только если имеется конкретная правовая основа (согласие, общественный интерес и т.п.). Кроме того, сообщайте персональные данные другим организациям или органам власти, только если они соблюдают адекватные нормы по защите данных, соответствующие, по меньшей мере, тем же стандартам, что и | Уровень риска достаточно снижен<br><br>Уровень риск не обязательно снижен, но риск принимается<br><br>Уровень риска не снижен и риск не принимается |

| Вопрос, связанный с защитой данных | Кодекс поведения | Оценка рисков | Меры по снижению риска | Вывод |
|---|---|---|---|---|
| защиты данных?<br><br>Согласился ли субъект данных явным образом с тем, что вы сообщите еще кому-то его персональные данные?<br><br>Если ваша организация создает рекламные видео, брошюры или передает истории в прессу, делаете ли вы анонимной информацию личного характера, чтобы даже если ее связать с другими данными, будет невозможно идентифицировать человека. | делу и обновленных данных<br><br>2.3.7 Безопасность данных<br><br>5. Опубликование | ➢ Субъект данных / его семья может подвергнуться опасности, если организация не обрабатывает данные в соответствии с адекватными стандартами по защите данных<br><br>➢ Отдельные лица могут подавать жалобы в связи с разглашением их персональных данных | Кодекс поведения в отношении ВСС.<br>▪ Опубликовывайте только фотографию и номер телефона центра, никаких других подробностей. Перепроверьте достоверность информации относительно предполагаемых родственников, сравнив ее с другими имеющимися данными или у самих бенефициариев до того, как принять запрос на восстановление связи. | |

| Вопрос, связанный с защитой данных | Кодекс поведения | Оценка рисков | Меры по снижению риска | Вывод |
|---|---|---|---|---|
| <u>Сохранение данных</u><br>Вводится ли информация личного характера в базы данных?<br><br>Необходимо ли сохранять все данные, которые обрабатываются?<br><br>Существуют ли процедуры для пересмотра времени сохранения данных?<br><br>Существуют ли политика, процедура или логическое обоснование архивирования информации личного характера?<br><br>Не слишком ли много данных хранится для целей аудита? Можно ли сократить этот объем? | 2.3.6 Сохранение данных | **Примеры:** первоначально собранные персональные данные собираются без указания периода их сохранения и хранятся в течение неограниченного времени.<br><br>**На практике**: большие объемы данных регистрируются в базах данных национальных обществ, но не обязательно служат для достижения цели, для которой они сначала собирались.<br><br>➢ Перегрузка информацией: в этом контексте управление данными занимает много времени, и, возможно, не стоит этого делать, если данные не являются необходимыми для выполнения деятельности по ВСС.<br><br>➢ Национальное общество не соблюдает Кодекс поведения | **Примеры:**<br>▪ Ограничение времени сохранения персональных данных периодом, необходимым для выполнения конкретных, ясных и законных целей.<br><br>▪ Использование базы данных: в рамках подхода, предусматривающего неприкосновенность частной жизни, указывайте в сопроводительном документе каждого файла период сохранения данных, а также соотнесите этот период с целью операций по обработке данных. Первоначально установленный период сохранения данных может быть продлен, если это будет сочтено необходимым для выполнения той задачи, для которой данные собирались. | Уровень риска достаточно снижен<br><br>Уровень риска не обязательно снижен, но риск принимается<br><br>Уровень риска не снижен и риск не принимается |

| Вопрос, связанный с защитой данных | Кодекс поведения | Оценка рисков | Меры по снижению риска | Вывод |
|---|---|---|---|---|
| | | | | |
| Риски для отдельных лиц иные, нежели риски, определенные выше: может ли сама по себе деятельность, о которой идет речь, привести к возникновению рисков для физической или психической неприкосновенности соответствующих лиц? | | | | |
| Подотчетность/механизмы контроля:<br><br>Эффективно ли соблюдаются стандарты и выполняются процедуры по защите данных?<br><br>Действуют ли механизмы, обеспечивающие контроль за существующей практикой и руководящие указания для национальных обществ? | 6. Применение Кодекса поведения в отношении ВСС | **Пример:** внутренняя угроза – Поскольку никто не может нести конкретную ответственность за сохранность персональных данных, сотрудники национального общества могут собирать и использовать персональные данные, не думая о последствиях своих действий.<br><br>**На практике:**<br>▪ Национальное общество, возможно, не поручило никому отвечать за отчетность в области защиты данных.<br>▪ Никто не подтвердил документами и не предоставил информацию о политике, процедурах и практике.<br>▪ Национальное общество не назначило конкретного сотрудника ответственным за | **Пример:** Контактному лицу в области защиты данных поручается конкретная обязанность обеспечить адекватность политики, процедур и практики национальных обществ в соответствии с Кодексом поведения в отношении ВСС | Уровень риска достаточно снижен<br><br>Уровень риска не обязательно снижен, но риск принимается<br><br>Уровень риска не снижен и риск не принимается |

| Вопрос, связанный с защитой данных | Кодекс поведения | Оценка рисков | Меры по снижению риска | Вывод |
|---|---|---|---|---|
| | | передачу персональных данных третьей стороне и не удостоверилось в том, что организация, которой оно сообщает персональные данные, соблюдает стандарты в области защиты данных в той же степени, что и требует Кодекс поведения в отношении BCC.<br><br>➢ Отсутствие доверия к деятельности, осуществляемой национальным обществом | | |