ПРАВИЛА МККК ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

СПРАВОЧНОЕ ИЗДАНИЕ

МККК

Приняты Директоратом МККК 24 февраля 2015 г. (с обновлениями от 10 ноября 2015 г.)
Последняя редакция принята Ассамблеей МККК 19 декабря 2019 г. и 10 апреля 2025 г.

СОДЕРЖАНИЕ

ПРЕАМБУЛА

ОБЩАЯ ИНФОРМАЦИЯ

Законодательство в области защиты данных в последние годы развивается очень быстро: более чем в 130 странах сейчас имеются законы о защите данных или какие-либо законодательные требования относительно неприкосновенности частной жизни. Продолжают разрабатываться и новые законы, по мере того как мир осознает необходимость защиты данных.

С развитием новых технологий и ростом уровня взаимных связей в мире, позволяющих быстрее и легче обрабатывать все увеличивающийся объем данных, повышается вероятность вторжения в личную сферу жизни частных лиц. Это не осталось незамеченным, и по всему миру принимаются меры для решения этой проблемы.

Международный Комитет Красного Креста (МККК) признает огромный потенциал этих изменений для своей гуманитарной деятельности и стремится встроить их в ее структуру. В то же время он ясно осознает сопутствующие риски, а также важность разработки надлежащих стандартов в области защиты данных и введения их в действие.

Защита персональных данных частных лиц, особенно в условиях таких испытаний, как вооруженные конфликты и прочие чрезвычайные ситуации гуманитарного характера, — важный аспект защиты жизни людей, их физической и психической неприкосновенности, их достоинства, что делает ее вопросом чрезвычайной важности для МККК. Она касается всех областей деятельности МККК — как оперативного, так и административного характера.

В результате МККК принял следующий свод правил в области защиты персональных данных, что позволит ему также сохранить лидирующие позиции в области гуманитарной деятельности даже в самых сложных ситуациях.

ЦЕЛЬ

Настоящие правила призваны дать МККК возможность осуществлять его мандат в соответствии с нормами международного гуманитарного права (МГП) и Уставом Международного движения Красного Креста и Красного Полумесяца (Уставом Движения), а также с любыми необходимыми административными процедурами, соблюдая при этом международно признанные стандарты защиты персональных данных.

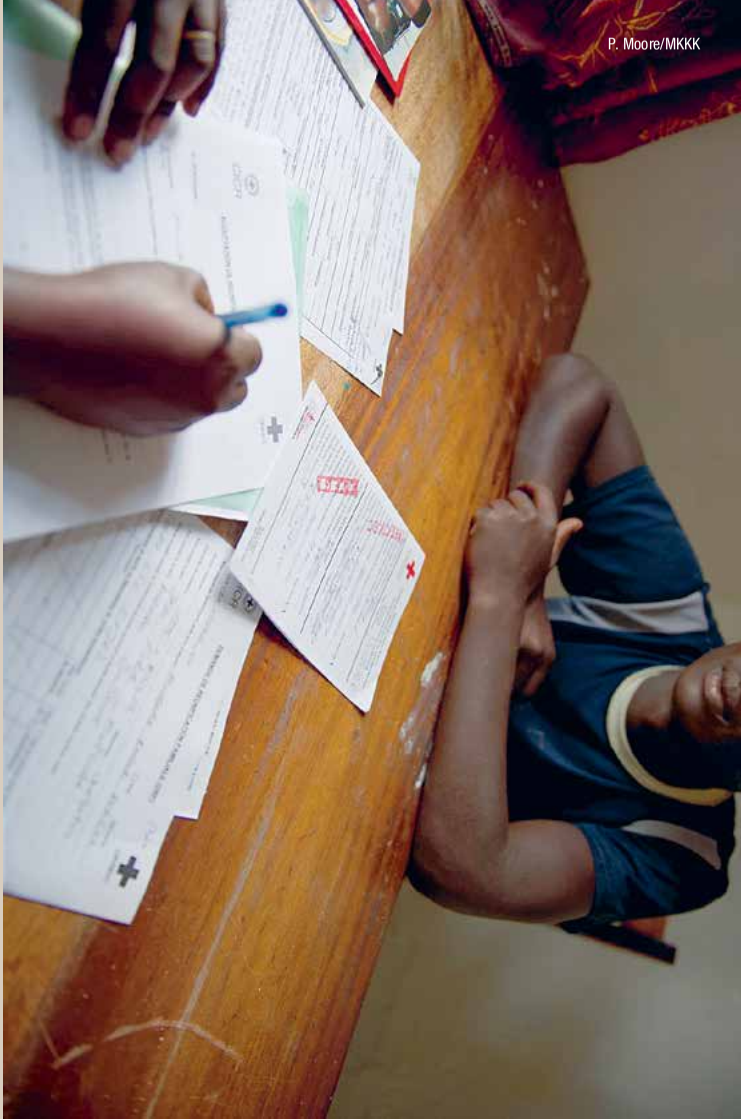
Они применяются исключительно к обработке персональных данных. Определения терминов, используемых в тексте настоящих правил, приведены в Приложении.

МАНДАТ МККК В ОБЛАСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Главный мандат МККК в области обработки персональных данных основан на положениях МГП и Устава Движения, в соответствии с которыми в нем формулируется задача по предоставлению защиты и оказанию помощи людям во время вооруженных конфликтов и в других ситуациях насилия.

МККК работает в рамках своего гуманитарного мандата в полном соответствии со своими Основополагающими принципами (в особенности принципами гуманности, беспристрастности, нейтральности и независимости) и своими стандартными методами работы, которые включают в себя, в частности, соблюдение конфиденциальности.

Для сохранения нейтрального, беспристрастного и независимого характера деятельности МККК и в соответствии с исключительно гуманитарными целями такой деятельности обработка персональных данных в МККК регулируется исключительно данными правилами, независимый надзор над такой обработкой осуществляет Бюро МККК по защите данных, а Независимая контрольная комиссия МККК по защите данных (Комиссия МККК по защите данных) обеспечивает эффективные средства правовой защиты.


P. Moore/MKKK

ГЛАВА 1
ОСНОВНЫЕ ПРИНЦИПЫ

СТАТЬЯ 1. ЗАКОННАЯ И ДОБРОСОВЕСТНАЯ ОБРАБОТКА ДАННЫХ

1. МККК осуществляет обработку персональных данных в соответствии с принципами, приведенными в данной главе.

2. МККК осуществляет обработку персональных данных только при наличии законных оснований для этого, указанных в настоящих правилах. К числу законных оснований, которые могут применяться для обработки данных, относятся следующие:
   a) согласие субъекта данных;
   b) жизненно важные интересы субъекта данных или другого лица;
   c) общественный интерес, в частности обусловленный мандатом МККК в соответствии с МГП и (или) Уставом Движения;
   d) законные интересы МККК — при условии, что над этими интересами не имеют приоритета права и свободы субъектов данных;
   e) выполнение контракта;
   f) выполнение правового обязательства.

3. МККК проявляет особую осмотрительность при обработке персональных данных определенных особо уязвимых категорий субъектов данных, таких как дети, люди преклонного возраста, лица с социально-психологическими или умственными нарушениями или перенесшие психологическую травму.

4. МККК также проявляет особую осмотрительность при обработке конфиденциальных данных.

СТАТЬЯ 2. ПРОЗРАЧНАЯ ОБРАБОТКА ДАННЫХ

1. Обработка данных должна быть прозрачной для субъектов данных, которых она касается. Субъекты данных должны получить определенный минимум информации об обработке, как сказано в статье 7 ниже. Приняв во внимание такие факторы, как условия безопасности на местах, логистические ограничения и степень срочности осуществления обработки, ответственное лицо МККК определяет, каким образом будет передаваться эта информация. Субъекты данных должны получать эту информацию по сути во время сбора их персональных данных или при первой возможности.

2. Кроме того, вся информация и обмен сообщениями, касающиеся обработки данных, должны быть доступными и понятными. Необходимо использовать ясный и простой язык.

СТАТЬЯ 3. ОБРАБОТКА ДЛЯ КОНКРЕТНЫХ ЦЕЛЕЙ / ДАЛЬНЕЙШАЯ ОБРАБОТКА

1. При сборе данных ответственное лицо МККК определяет конкретную и законную цель (цели) обработки информации; обработка информации осуществляется только с этой целью (целями). Цели обработки персональных данных, находящиеся в рамках гуманитарного мандата МККК, включают в себя:
   a) защиту семейных связей;
   b) защиту лиц, находящихся в местах содержания под стражей;
   c) защиту гражданского населения;
   d) повышение уровня соблюдения МГП, в том числе путем проведения обучения и укрепления потенциала;
   e) предоставление медицинской помощи;
   f) деятельность в области судебной медицины;
   g) устранение оружейной опасности;
   h) обеспечение экономической безопасности;
   i) защиту систем водоснабжения и водоотведения;
   j) профилактическую и терапевтическую медицину.

2. Приемлемыми также считаются цели, связанные с конкретной законной деятельностью, необходимой для выполнения мандата

МККК, включая любые административные задачи (такие, как работа с персоналом и любая финансовая деятельность).

3. МККК может осуществлять обработку персональных данных для целей, отличных от тех, которые были определены во время сбора данных, если такая дальнейшая обработка совместима с этими исходными целями. Чтобы убедиться, что дальнейшая обработка данных совместима с первоначальной целью (целями), контролер данных должен учитывать, среди прочего, связь между первоначальной целью (целями) и целью (целями) дальнейшей обработки данных; обстоятельства сбора персональных данных, включая разумные ожидания субъектов данных, а также потенциальные последствия дальнейшей обработки для субъектов данных. Однако дальнейшая обработка недопустима, если угроза интересам, правам и свободам субъектов данных превосходит преимущества дальнейшей обработки персональных данных.

4. Предполагается, что дальнейшая обработка персональных данных, необходимая с исторической, статистической, научной точки зрения или для отчетности о гуманитарной деятельности, соответствует первоначальным целям МККК по обработке данных.

5. Субъекты данных должны быть как можно раньше проинформированы о дополнительных целях и дальнейшей обработке в соответствии со статьей 2.

СТАТЬЯ 4. НАДЛЕЖАЩИЕ, АКТУАЛЬНЫЕ И НЕ ЯВЛЯЮЩИЕСЯ ИЗЛИШНИМИ ДАННЫЕ

1. Данные, с которыми работает МККК, должны быть надлежащими, актуальными для тех целей, которые преследуются при их сборе и обработке, и должны ограничиваться ими.

2. Собранные данные не должны быть излишними для целей сбора и должны быть пригодны для дальнейшей обработки. Период, в течение которого данные хранятся, прежде чем будут анонимизированы, архивированы или удалены, не должен быть более продолжительным, чем это необходимо.

СТАТЬЯ 5. КАЧЕСТВО ДАННЫХ

1. Персональные данные должны быть в максимальной степени точными и обновленными.

2. Необходимо принять все разумные меры предосторожности, чтобы обеспечить исправление или удаление персональных данных, признанных неточными, без необоснованной задержки (с учетом целей их обработки).

СТАТЬЯ 6. ХРАНЕНИЕ, УДАЛЕНИЕ И АРХИВИРОВАНИЕ ДАННЫХ, В КОТОРЫХ БОЛЬШЕ НЕТ НЕОБХОДИМОСТИ

1. Чтобы данные не хранились дольше, чем это необходимо, устанавливается минимальный период хранения, в конце которого проводится оценка с целью выяснения, есть ли дальнейшая необходимость в этих данных. В зависимости от результатов оценки период хранения продлевается или данные удаляются / архивируются.

2. Данные должны удаляться в следующих случаях:
   a) они больше не являются необходимыми для целей, которые преследовались при их сборе или дальнейшей обработке;
   b) субъекты данных отзывают свое согласие на обработку, при этом согласие является правовой основой для обработки;
   c) субъекты данных возражают против обработки данных, и их возражения поддерживает ответственное лицо МККК или Комиссия МККК по защите данных;
   d) настоящие правила иным образом предусматривают удаление данных.

3. Однако данные не должны удаляться, когда есть законная причина для их архивирования, например, данные могут потребоваться для долговременного предоставления гуманитарных услуг, они могут быть необходимы с исторической, статистической и научной точки зрения или для отчетности о гуманитарной деятельности.

T. Gassmann/MKKK

ГЛАВА 2
ПРАВА СУБЪЕКТОВ ДАННЫХ

СТАТЬЯ 7. ИНФОРМАЦИЯ

1. Следующий минимум информации об обработке данных должен предоставляться субъектам данных (устно или письменно, в простой, доступной для понимания форме) при получении или сборе данных:
   a) является ли МККК контролером данных, и есть ли другие контролеры данных;
   b) основные элементы мандата МККК и, если применимо, других контролеров данных;
   c) цель (цели) обработки данных;
   d) категории собранных персональных данных;
   e) вероятность того, что данные будут направлены получателям за пределами организации (в одно или несколько национальных обществ Красного Креста или Красного Полумесяца и (или) в любые другие организации);
   f) информация о применении автоматизированных систем принятия решений и профилирования, о которых говорится в ст. 12, и — по крайней мере в случае их использования — содержательная информация о применяемой логике, а также о значимости и предполагаемых последствиях такой обработки для субъекта данных;
   g) наличие права запросить у контролера (контролеров) данных доступ к персональным данным, исправить или удалить их, а также возможность возразить против их обработки в соответствии с настоящими правилами; если обработка проводится на основании согласия, необходимо также сообщить о наличии права отозвать согласие в любое время;
   h) информация о том, что субъекты данных могут адресовать все вопросы / соображения / жалобы, касающиеся работы с их данными, любому сотруднику МККК, сотруднику Бюро МККК по защите данных или непосредственно в Комиссию МККК по защите данных;
   i) продолжительность периода хранения данных.

Если МККК не в состоянии (по причинам логистического характера или из соображений безопасности) предоставить такую информацию при получении или сборе персональных данных, он должен предоставить ее позже без необоснованной задержки.

2. Когда источником получения данных не является непосредственно субъект данных, такая информация должна предоставляться в течение разумного периода в устном или письменном виде с учетом соображений безопасности и логистических ограничений, с которыми сталкивается МККК. Очень важно в каждом случае проследить, чтобы информация, предоставляемая субъектам данных, не причинила им вреда, ущерба или психологических страданий.

3. Если МККК не может предоставить субъекту данных эту информацию, он должен принять соответствующие меры по защите прав, свобод и законных интересов субъекта данных, в том числе обнародовать эту информацию.

СТАТЬЯ 8. ДОСТУП

1. Субъекты данных должны иметь возможность получать по запросу, с разумной периодичностью и без излишней задержки подтверждение обработки касающихся их персональных данных и всю необходимую информацию об обработке. Такая информация включает в себя цель (цели) обработки; соответствующие категории персональных данных; предполагаемый срок хранения данных; третьи стороны, которым данные будут передаваться, если таковые есть; источник персональных данных; права субъектов данных и то, как их осуществлять. Сведения об обработанных данных должны предоставляться субъектам данных в понятной форме. Субъекты данных также должны иметь возможность проверить свои персональные данные и должны иметь доступ к ним за исключением случаев, указанных в пункте 3 ниже.

2. Раскрытие персональных данных не должно происходить автоматически. Ответственное лицо МККК должно сначала рассмотреть все обстоятельства, связанные с запросом на допуск, включая любые признаки того, что запрос мог быть сделан под давлением или принуждением, и проанализировать все применимые ограничения. Сотрудники МККК никогда не должны

раскрывать информацию о субъектах данных, кроме случаев, когда имеются достаточные доказательства того, что лицо, запрашивающее информацию, является субъектом данных.

3. Право доступа к документам не применяется в случаях, когда важные общественные интересы требуют отказа в доступе. К таким интересам относятся:
   a) обеспечение конфиденциальности, которая является важнейшей характеристикой работы МККК;
   b) обеспечение эффективности деятельности, осуществляемой в рамках мандата МККК;
   c) сохранение конфиденциальности взглядов или суждений сотрудников МККК, нарушение которой может поставить под угрозу операции МККК и (или) привести к раскрытию персональных данных сотрудников;
   d) права и свободы других лиц, которые имеют приоритет над интересами субъекта данных.

4. Запросы от родителей и законных опекунов должны в максимальной степени отражать интересы ребенка или уязвимого субъекта данных. Предполагается, что доступ соответствует таким интересам, когда осуществляется родителями или законными опекунами. Однако ответственное лицо МККК может отказать в раскрытии персональных данных ребенка или уязвимого субъекта данных, если имеются достаточные основания полагать, что это не будет отвечать интересам конкретного ребенка или уязвимого субъекта данных.

5. Законным является стремление людей к воссоединению со своими родственниками, направление запросов с целью выяснения местонахождения и участи субъектов данных, являющихся их родственниками, а также изучение семейной истории, особенно если члены семьи были разлучены в результате вооруженного конфликта или других ситуаций насилия. Запросы на получение данных по вышеуказанным причинам являются законными, однако при этом необходимо учитывать вопросы соблюдения конфиденциальности, а также права и интересы субъектов данных.

6. Доступ к архивным данным осуществляется при строгом соблюдении условий и процедур, которые установлены в Правилах доступа к архивам МККК.

СТАТЬЯ 9. ИСПРАВЛЕНИЕ

По просьбе субъекта данных ошибки или неточности в его персональных данных должны быть исправлены ответственным лицом МККК, за исключением следующих случаев:

a) личность субъекта данных не может быть проверена ответственным лицом МККК;
b) просьба о внесении исправлений касается оценки, проведенной сотрудниками МККК, и субъект данных не может предоставить достаточные доказательства неточности оценки;
c) данные содержатся в документах, находящихся в архивах МККК; в этом случае в соответствующее архивное дело может быть включено примечание о том, что был сделан запрос на внесение исправлений.

СТАТЬЯ 10. УДАЛЕНИЕ

1. Субъект данных должен иметь возможность настоять на удалении своих персональных данных из активных баз данных МККК по причинам, перечисленным в пункте 2 статьи 6 настоящих правил.

2. Однако право на удаление не применяется и персональные данные будут продолжать храниться в следующих случаях:
   a) когда у ответственного лица МККК имеются опасения, что просьба субъекта данных об удалении продиктована внешним давлением и что удаление данных нанесет вред интересам этого субъекта данных или другого лица;
   b) по причинам, связанным с правом на свободу волеизъявления / свободу информации, в том числе в целях документирования деятельности МККК в соответствии с политикой конфиденциальности организации;
   c) если того требует общественный интерес;
   d) в исторических, статистических и научных целях;
   e) в долгосрочных гуманитарных целях или для установления ответственности;
   f) для подачи и исполнения судебных исков или защиты по таковым.

СТАТЬЯ 11. ВОЗРАЖЕНИЕ

1. Субъект данных может в любое время возразить против обработки касающихся его персональных данных, имея для этого веские законные основания применительно к его ситуации.

2. Такое возражение будет принято, если интересы, основные права и свободы субъекта данных, о котором идет речь, перевешивают законные интересы МККК или общественный интерес в обработке данных.

СТАТЬЯ 12. АВТОМАТИЗИРОВАННОЕ ПРИНЯТИЕ РЕШЕНИЙ И ПРОФИЛИРОВАНИЕ

1. МККК не должен принимать решение, используя исключительно автоматизированные системы принятия решений, если такое решение имеет правовые последствия для субъекта данных и (или) серьезно вредит ему, за исключением случаев, когда такая обработка происходит с согласия субъекта данных или необходима для выполнения договора между субъектом данных и МККК.

2. МККК не должен принимать решение, основываясь исключительно на профилировании, когда такое решение имеет правовые последствия для субъекта данных и (или) серьезно вредит ему, за исключением случаев, когда такая обработка происходит с согласия субъекта данных.

3. МККК должен принимать необходимые меры, чтобы защищать права, свободы и законные интересы субъекта данных, как минимум право обратиться к сотрудникам МККК, право на выражение своей точки зрения и на оспаривание решений, о которых говорится в пунктах 1 и 2 статьи 12.

СТАТЬЯ 13. ОТСТАИВАНИЕ ЧАСТНЫМИ ЛИЦАМИ ПРАВ НА ЗАЩИТУ ДАННЫХ

1. Субъекты данных могут официально заявить о своих правах на защиту данных, обратившись в Бюро МККК по защите данных — напрямую или через любого сотрудника МККК.

2. Когда Бюро МККК по защите данных не может удовлетворить жалобу лица самостоятельно, оно должно направить дело в Комиссию МККК по защите данных.

3. Если Бюро по защите данных не передало дело в Комиссию по защите данных, субъект данных может направить официальное заявление о своих правах на защиту данных напрямую в Комиссию по защите данных.

4. Если жалоба будет сочтена обоснованной, должны быть приняты соответствующие меры.

СТАТЬЯ 14. ОТСТУПЛЕНИЕ ОТ ПРАВИЛ

Если под угрозой оказывается гуманитарный мандат МККК по предоставлению защиты и помощи людям, пострадавшим от вооруженных конфликтов и других ситуаций насилия, либо его независимость, беспристрастность или нейтральность, или если существует вероятность нарушения эффективной деятельности МККК, Директорат МККК может принять временные меры в отношении обработки данных, необходимые и применимые в таких обстоятельствах, после проведения консультаций с Бюро МККК по защите данных и главой соответствующего управления МККК.


N. Kero/MKKK

ГЛАВА 3

ОБЯЗАТЕЛЬСТВА МККК

СТАТЬЯ 15. ОТВЕТСТВЕННОСТЬ / ОТЧЕТНОСТЬ

1. Контролер данных должен убедиться, что приняты все необходимые меры, позволяющие гарантировать и продемонстрировать, что обработка персональных данных от его собственного имени или через субподрядчика соответствует настоящим правилам.

2. Ответственное лицо МККК отвечает за то, чтобы все, кто имеет доступ к персональным данным и подчиняется МККК, работали с данными (занимались их обработкой) в соответствии с этими правилами и политикой защиты данных, одобренной Директоратом и (или) Ассамблеей МККК.

3. В соответствии с этим, когда МККК сотрудничает в области обработки данных с другой организацией, обязанности всех сторон должны быть очень четко определены и закреплены контрактом или другой юридически обязательной договоренностью. Например, организация, которая приступает к обработке персональных данных от имени МККК (обработчик данных), должна дать согласие на осуществление определенных мер по защите данных, а также на обработку данных исключительно в соответствии с указаниями МККК. Если это не представляется возможным и если ответственное лицо МККК придерживается мнения, что обработка данных все равно должна быть осуществлена, этот факт должен быть учтен при проведении оценки последствий обработки данных (см. статью 17).

СТАТЬЯ 16. ЗАЩИТА ДАННЫХ, ОБЕСПЕЧИВАЕМАЯ НА КОНСТРУКТИВНОМ УРОВНЕ И ПО УМОЛЧАНИЮ

При проектировании базы данных или другого инструмента для обработки данных или при разработке порядка сбора персональных данных все эти правила должны быть учтены и интегрированы в максимально возможной степени. Это называется «защита данных, обеспечиваемая на конструктивном уровне и по умолчанию».

СТАТЬЯ 17. ОЦЕНКА ПОСЛЕДСТВИЙ ОБРАБОТКИ ДАННЫХ

1. Когда существует вероятность того, что обработка данных будет связана с высокими рисками для прав и свобод субъектов данных, ответственное лицо МККК будет отвечать за проведение — до начала обработки данных — оценки последствий предполагаемых операций по обработке для защиты персональных данных (оценка последствий обработки данных). В условиях чрезвычайных ситуаций это можно сделать после обработки, однако в максимально сжатые разумные сроки.

2. При оценке того, будет ли связана обработка данных с высокими рисками для прав и свобод субъектов данных, ответственное лицо МККК в тесном взаимодействии с Бюро по защите данных должны рассмотреть такие факторы, как масштаб, характер, охват и страна или регион, где проводится обработка данных (например, проводится ли обработка конфиденциальных данных или данных особо уязвимых субъектов данных, включая детей и пожилых людей), но не ограничиваться ими.

3. При проведении оценки последствий обработки данных должны использоваться стандартные формы и инструкции, подготовленные Бюро МККК по защите данных. Такая оценка будет служить основанием для возможного применения смягчающих мер. Необходимо проводить консультации с Бюро МККК по защите данных: оно может давать указания относительно смягчающих мер и их применения.

СТАТЬЯ 18. ДОКУМЕНТИРОВАНИЕ ОБРАБОТКИ ДАННЫХ

В целях демонстрации соблюдения настоящих правил ответственное лицо должно вести журнал учета действий по обработке данных, особенно тех категорий действий, которые относятся к его компетенциям. Эта работа ведется под контролем Бюро МККК по защите данных.

СТАТЬЯ 19. СОТРУДНИЧЕСТВО С НАДЗОРНЫМИ ОРГАНАМИ

1. Любое сотрудничество с национальными или региональными органами, отвечающими за защиту данных, всегда осуществляется без ущерба для привилегий и иммунитета МККК, предусмотренных внутригосударственным законодательством и международным

правом. Для обеспечения полной защиты персональных данных субъекта данных МККК должен убедиться, что его особый статус признан и что все заинтересованные стороны уведомлены о том, что МККК нельзя принуждать к раскрытию информации, полученной в ходе его деятельности. Если говорить конкретнее, должно уважаться право МККК на неразглашение информации.

2. Любая просьба надзорного органа в области защиты данных о сотрудничестве или предоставлении информации о любом субъекте данных должна направляться в Бюро МККК по защите данных, прежде чем она будет удовлетворена.

СТАТЬЯ 20. НАРУШЕНИЕ БЕЗОПАСНОСТИ ДАННЫХ

1. О любом нарушении безопасности, которое ведет к случайному или противозаконному уничтожению, потере или изменению передаваемых, хранящихся или иным образом обрабатываемых персональных данных или к неправомерному раскрытию таких данных либо получению доступа к ним, необходимо всегда сообщать в Бюро МККК по защите данных.

2. Лица, затронутые в результате утечки данных, должны быть уведомлены о такой утечке ответственным лицом в тесном взаимодействии с Бюро по защите данных без необоснованной задержки, когда такая утечка представляет для них особенно серьезный риск, за исключением случаев, когда:
   a) это связано с несоразмерными усилиями, обусловленными логистическими условиями, условиями безопасности или количеством дел, о которых идет речь; в таких случаях ответственное лицо МККК в тесном взаимодействии с Бюро МККК по защите данных должно решить, будет ли уместно сделать публичное заявление или прибегнуть к аналогичной мере, чтобы проинформировать всех субъектов данных одинаково эффективно;
   b) это окажет негативное воздействие на предмет, представляющий значительный общественный интерес, например на эффективность операций МККК;
   c) в связи с ситуацией, сложившейся в сфере безопасности, контакт с субъектами данных может подвергнуть их опасности или вызвать у них серьезное потрясение.

СТАТЬЯ 21. БЕЗОПАСНОСТЬ ДАННЫХ

1. Персональные данные должны обрабатываться таким образом, чтобы обеспечивался надлежащий уровень безопасности согласно Руководству МККК по обеспечению безопасности информации и соответствующей политике и стандартам. Это включает в себя обеспечение доступа к персональным данным в соответствии со строгими правилами, определяющими, кому необходимо быть ознакомленным с той или иной информацией, но не ограничивается этим. При определении необходимого уровня безопасности учитывается ряд факторов, однако особое внимание необходимо уделить таким показателям, как характер, охват, страна или регион и цель обработки данных, а также опасность, которая может угрожать субъектам данных и мандату МККК. Сюда входит предотвращение незаконного доступа к персональным данным и оборудованию для их обработки, а также их незаконного использования. В частности, это касается прав доступа к базам данных, физической безопасности, компьютерной безопасности или кибербезопасности, обязанности соблюдать конфиденциальность и поведения сотрудников.

2. Когда хранение персональных данных больше не является необходимым, все записи и резервные копии должны быть надежным образом уничтожены или анонимизированы.

D. Revol/MKKK

ГЛАВА 4
ПЕРЕДАЧА ДАННЫХ

СТАТЬЯ 22. ТРЕБОВАНИЯ К ПЕРЕДАЧЕ ДАННЫХ

1. Данные могут передаваться организациям за пределами МККК только при соблюдении следующих условий:
   a) установлено применимое законное основание для передачи:
      i) согласие субъекта данных;
      ii) жизненно важные интересы субъекта данных или другого лица;
      iii) общественный интерес, в частности, обусловленный мандатом МККК в соответствии с нормами МГП и (или) Уставом Движения;
      iv) законные интересы МККК — при условии, что над этими интересами не имеют приоритета права и свободы субъектов данных;
      v) выполнение контракта;
      vi) выполнение правового обязательства;
   b) проведена оценка рисков и приняты соответствующие смягчающие меры в соответствии со статьей 23; в зависимости от степени конфиденциальности ситуации и риска, который передача представляет для отдельных лиц или для МККК, может потребоваться проведение полной оценки последствий обработки данных в отношении передаваемых персональных данных;
   c) обработка данных получателем в максимальной степени ограничена конкретными целями обработки в интересах МККК или допустимой дальнейшей обработки;
   d) количество и тип персональных данных, предназначенных для передачи, строго ограничены тем, что необходимо знать получателю для конкретных целей или для предполагаемой дальнейшей обработки;
   e) передача данных совместима с разумными ожиданиями субъекта данных;
   f) приняты соответствующие меры по обеспечению защиты передачи персональных данных третьим сторонам; средства передачи и применяемые методы обеспечения

безопасности должны соответствовать характеру и уровню конфиденциальности персональных данных, рискам, выявленным в ходе оценки рисков, и степени срочности действий гуманитарного характера;

g) ведется журнал учета передачи персональных данных.

СТАТЬЯ 23. СОГЛАШЕНИЯ О ПЕРЕДАЧЕ ДАННЫХ

1. Для систематических и масштабных передач данных, а также в тех случаях, когда речь идет о передаче особо конфиденциальных данных, — и в зависимости от того, насколько срочно необходимо обработать данные, — требуется официальное соглашение между получателем и контролером данных. Речь может идти об отдельных пунктах, касающихся безопасности и защиты данных, в соглашении о партнерстве или меморандуме о взаимопонимании либо об отдельном соглашении о передаче данных.

2. При передаче данных, не подпадающей под такого рода соглашения, должны быть приняты следующие меры:
   a) получатель в письменной форме обязуется обрабатывать персональные данные только в тех конкретных целях, для которых они были переданы, или проводить дальнейшую обработку, совместимую с такими целями, и не передавать их третьим лицам без предварительного согласия МККК;
   b) ответственное лицо МККК должно убедиться, что получатель принял технические и организационные меры для надлежащей защиты передаваемых персональных данных.

3. До подписания любых подобных соглашений, договорных положений, письменных обязательств или аналогичных правовых документов необходимо проконсультироваться с Бюро МККК по защите данных.

СТАТЬЯ 24. ЗАПРОСЫ СО СТОРОНЫ ВЛАСТЕЙ

1. Любое использование привилегий и иммунитетов МККК, включая право МККК на неразглашение информации, должно всегда уважаться, и все ответы на запросы органов власти о доступе к персональным данным, хранящимся в МККК, должны заранее

согласовываться с Бюро МККК по защите данных для обеспечения оптимальной защиты соответствующих персональных данных.

2. Данные должны предоставляться органам власти, сторонам в вооруженном конфликте или акторам, вовлеченным в иные ситуации насилия, только после подтверждения (полученного в ходе "оценки рисков" ответственным лицом МККК или всеобъемлющей оценки эффективности защиты данных), что передача этой информации с малой вероятностью приведет к возникновению несоразмерных рисков для личной безопасности субъекта данных, безопасности его семьи или его окружения или для МККК.

СТАТЬЯ 25. ДОСТУП К ДАННЫМ ПО АДМИНИСТРАТИВНЫМ ПРИЧИНАМ ИЛИ ДЛЯ ПРОВЕДЕНИЯ ГЕНЕАЛОГИЧЕСКОГО ИССЛЕДОВАНИЯ

Ответственное лицо МККК может рассмотреть возможность раскрытия персональных данных третьей стороне, разыскивающей субъекта данных, или родственникам субъекта данных, запрашивающим доступ к архивам МККК по административным причинам или для проведения генеалогического исследования. Однако в обоих случаях решение о раскрытии данных принимается с учетом условий, указанных в настоящей главе, а также условий и процедур, указанных в правилах доступа к архивам МККК, если применимо.

C. Brueser/MKK

ГЛАВА 5
ВЫПОЛНЕНИЕ

СТАТЬЯ 26. ЭФФЕКТИВНОЕ ВЫПОЛНЕНИЕ

1. Эффективное выполнение этих правил крайне важно для обеспечения возможности субъектов данных пользоваться предоставляемой ими защитой. Эффективное выполнение обеспечивается усилиями ответственного лица МККК, Бюро МККК по защите данных и Комиссией МККК по защите данных.

2. Именно на ответственное лицо МККК, находящееся в подчинении главы делегации в структурах МККК на местах и соответствующему директору в штаб-квартире МККК, возложена задача обеспечить выполнение данных правил и политики МККК в отношении защиты данных.

3. Чтобы эффективно применять настоящие правила, Бюро МККК по защите данных должно иметь свободный неограниченный доступ ко всем документам, данным и системам для обработки такой информации, независимо от места, способа или средства обработки. Такой доступ должен ограничиваться по мере необходимости и, насколько это возможно, предоставляться Бюро МККК по защите данных таким образом, чтобы не препятствовать ежедневной работе ответственного лица МККК. Если ответственное лицо МККК оспаривает необходимость доступа к документам, данным или системам, оно должно иметь возможность передать рассмотрение данного вопроса на более высокий уровень с учетом охвата и характера проблемы.

4. Отделы штаб-квартиры МККК в Женеве и структуры МККК на местах, работающие под руководством соответствующего директора в штаб-квартире и главы делегации в структурах МККК на местах, отвечают за разработку целесообразных и эффективных мер, гарантирующих соответствие их деятельности принципам и обязательствам, изложенным в настоящих правилах.

5. Информация о возможных случаях несоблюдения этих правил должна немедленно направляться ответственному лицу МККК, которое должно расследовать их без необоснованной задержки. Если основания для жалобы подтверждаются, необходимо принять соответствующие меры, чтобы снизить риск причинения вреда субъекту данных.

6. Бюро МККК по защите данных должно направлять информацию о любых нарушениях этих правил, приведших к причинению вреда субъектам данных, в кадровый отдел штаб-квартиры МККК и в структуры на местах. В отношении сотрудников МККК, допустивших серьезные нарушения, могут быть приняты меры дисциплинарного характера.

СТАТЬЯ 27. БЮРО МККК ПО ЗАЩИТЕ ДАННЫХ

1. Субъект данных, который считает, что его права, установленные данными правилами, были нарушены, может направить жалобу в Бюро МККК по защите данных.

2. Если бюро не может найти решение, оно должно направить дело в Комиссию МККК по защите данных.

3. Если возникают вопросы, связанные с соблюдением условий обработки данных, Бюро МККК по защите данных должно проконсультироваться со структурами МККК на местах или, если действие происходит в штаб-квартире в Женеве, с соответствующим отделом для получения разъяснений или дополнительной информации, которая может прояснить вопрос. Бюро МККК по защите данных совместно с соответствующими структурами на местах или соответствующим отделом должно также принять дальнейшие меры, необходимые для выполнения этих условий. Бюро МККК по защите данных должно информировать и консультировать ответственное лицо МККК о его обязанностях в соответствии с настоящими правилами. Оно также должно документировать эти действия и реакцию на них.

4. Также Бюро МККК по защите данных отвечает за следующее:
   a) составление руководств с целью прояснения значения и случаев применения данных правил при необходимости;

b) контроль выполнения этих правил в отношении защиты данных, обеспечиваемой на конструктивном уровне и по умолчанию;
c) контроль соответствия настоящим правилам работы по проведению оценки последствий обработки данных, осуществляемой ответственными лицами МККК или обработчиком;
d) контроль ведения журнала учета всех видов действий по обработке данных в рамках своих полномочий;
e) разработку учебных модулей;
f) распространение информации по вопросам защиты данных среди сотрудников МККК;
g) контроль за выполнением данных правил и обеспечение их соблюдения.

5. Когда имеется срочная необходимость в действиях, направленных на защиту прав и свобод субъектов данных, Бюро МККК по защите данных имеет право ввести временные меры с установленным сроком.

6. Бюро МККК по защите данных не получает никаких указаний относительно выполнения упомянутых выше задач или предоставления рекомендаций и должно иметь возможность выполнять свои обязанности и задачи независимо. Сотрудников Бюро МККК по защите данных нельзя уволить или наказать каким-либо другим способом за исполнение их обязанностей. Бюро МККК по защите данных должно иметь возможность на регулярной основе связываться непосредственно с руководством МККК самого высокого уровня.

СТАТЬЯ 27BIS. ПРЕДСТАВИТЕЛИ БЮРО МККК ПО ЗАЩИТЕ ДАННЫХ

1. В каждой делегации по согласованию с Бюро МККК по защите данных и в соответствии с любыми особыми указаниями, которые могут поступить от Бюро МККК по защите данных в связи с этим, должен быть назначен представитель по вопросам защиты данных. Это необходимо для обеспечения того, чтобы каждая структура МККК на местах применяла настоящие правила и

механизмы, предусмотренные в них, при обработке любых данных, осуществляемой в рамках ее деятельности. Этот представитель должен иметь всеобъемлющую роль и заниматься любыми операциями по обработке персональных данных в структуре МККК на местах.

2. Каждый директор по согласованию с Бюро МККК по защите данных и в соответствии с любыми особыми указаниями, которые могут поступить от Бюро МККК по защите данных в связи с этим, должен также назначить представителя по вопросам защиты данных в своем отделе, чтобы обеспечить выполнение в каждом отделе штаб-квартиры настоящих правил и механизмов, которые предусматриваются в них, при обработке любых данных, осуществляемой в рамках их деятельности.

3. В частности, представитель по вопросам защиты данных:
   a) регулярно предоставляет точную отчетность по определенным базовым показателям, как это установлено Бюро МККК по защите данных;
   b) обеспечивает, чтобы соответствующие документы, информация, руководства и указания Бюро МККК по защите данных были доступны, актуальны и распространялись в его зоне ответственности;
   c) выступает в роли контактного лица по всем вопросам, касающимся защиты данных в зоне своей ответственности, в том числе выступает как основное связующее звено с Бюро МККК по защите данных, организует визиты его представителей и содействует проведению оценки при необходимости;
   d) в зоне своей ответственности обеспечивает, чтобы субъект данных имел возможность подать жалобу по поводу обработки персональных данных, проводимой структурами МККК на местах или соответствующим отделом штаб-квартиры МККК, согласно настоящим правилам;
   e) в зоне своей ответственности обеспечивает, чтобы важные элементы защиты данных систематически доводились до сведения всех сотрудников структур МККК на местах или соответствующего отдела штаб-квартиры МККК;
   f) определяет необходимость проведения обучающих мероприятий в области защиты данных и передает

соответствующую информацию в Бюро МККК по защите данных;

g) обеспечивает надлежащее выполнение любых рекомендаций, составленных Бюро МККК по защите данных в связи с конкретной деятельностью по обработке данных в структуре МККК на местах или в соответствующем отделе штаб-квартиры МККК.

СТАТЬЯ 28. КОМИССИЯ МККК ПО ЗАЩИТЕ ДАННЫХ

1. Комиссия МККК по защите данных отвечает за толкование этих правил и за принятие решений относительно их выполнения или нарушения.

2. Когда Бюро МККК по защите данных направляет Комиссии дело или когда субъект данных обращается к ней с жалобой, Комиссия МККК по защите данных уполномочена изучить все факты, истолковать правила, имеющие отношение к вопросу, и вынести решение, обязательное к исполнению.

3. Консультативное заключение Комиссии МККК по защите данных запрашивается в отношении стратегий и принципов деятельности МККК, использования новых для МККК технологий, проведения сложных, систематических и (или) масштабных операций по обработке данных, если они оказывают или могут оказать неблагоприятное воздействие на права субъектов данных.

C. Von Toggenburg/MKKK

ГЛАВА 6
ПЕРЕСМОТР И ОБНОВЛЕНИЕ

СТАТЬЯ 29. ПЕРЕСМОТР И ОБНОВЛЕНИЕ НАСТОЯЩИХ ПРАВИЛ

1. Чтобы МККК мог своевременно реагировать на законодательные, социальные и технологические изменения в области защиты данных, настоящие правила должны пересматриваться Директоратом МККК, а затем — Ассамблеей МККК как минимум раз в три года.

2. Для содействия такому регулярному пересмотру правил Бюро МККК по защите данных представляет Ассамблее МККК ежегодный доклад. Этот доклад должен содержать оценку проблем, возникших в ходе применения настоящих правил, правовых и технологических изменений, а также изменений в отношении и подходах к обработке персональных данных со стороны государств, гуманитарных организаций и иных негосударственных акторов, которые имеют отношение к деятельности МККК.

3. По результатам регулярного пересмотра МККК соответственно обновляет данные правила.

ПРИЛОЖЕНИЕ

ОПРЕДЕЛЕНИЯ

Автоматизированная система принятия решений — система, которая принимает решения на основе автоматизированных логических заключений. Таким образом она осуществляет процесс, за который в ином случае отвечал бы человек.

Активные данные — все персональные данные, обрабатываемые МККК и не являющиеся архивными данными; **активная база данных** — база данных, содержащая активные данные.

Архивные данные — персональные данные, содержащиеся в документах, которые были переданы в архивный отдел МККК. Данный отдел работает с этими данными и (или) несет за них ответственность. Архивные данные перестают быть активными данными. Документы, содержащие архивные данные, представляют собой **документированные материалы** МККК и как таковые не могут быть удалены или изменены.

Биометрические данные — персональные данные, полученные в результате конкретной технической обработки информации, связанной с физическими, психологическими и поведенческими характеристиками физического лица, которые позволяют уникальным образом идентифицировать его.

Бюро МККК по защите данных — независимый контрольный орган, отвечающий за выполнение задач, определенных правилами МККК по защите персональных данных, и имеющий необходимые полномочия для этого. Не следует путать Бюро МККК по защите данных с отделом, который занимается данными в управлении МККК по предоставлению защиты.

Генетические данные — персональные данные, касающиеся генетических или наследственных характеристик лица, полученные в результате анализа биологического образца, взятого у такого лица, в частности путем проведения анализа хромосом, дезоксирибонуклеиновой кислоты (ДНК) или рибонуклеиновой кислоты (РНК), или путем проведения анализа любого другого генетического или унаследованного элемента, позволяющего получить эквивалентную информацию.

Данные о здоровье — данные, имеющие отношение к физическому или психическому здоровью человека и свидетельствующие напрямую или косвенно о состоянии его здоровья.
Персональные данные, касающиеся здоровья, включают в себя, в частности, следующее:

- данные, касающиеся физического или психического состояния субъекта данных;
- информацию о регистрации для получения услуг в области здравоохранения;
- номер или символ, присвоенный лицу для его индивидуальной идентификации в целях охраны здоровья;
- информацию, полученную в результате исследования части тела или биологической жидкости, включая генетические данные и биологические образцы;
- любую информацию о болезнях, инвалидности, психических и социально-психологических нарушениях, риске заболевания, медицинской истории или клиническом лечении либо информацию о физиологическом или медико-биологическом состоянии субъекта данных;
- любую информацию о травматическом опыте, который оказал негативное влияние на психическое состояние субъекта данных или привел к социально-психологическим расстройствам.

Контролер данных — физическое или юридическое лицо, которое в одиночку или совместно с другими лицами определяет цель (цели) и средства обработки персональных данных.

Конфиденциальные данные — персональные данные, которые могут нанести очень серьезный ущерб (например, стать причиной дискриминации или репрессий) субъектам данных или другим лицам при неправильном обращении с такими данными или их раскрытии. Квалификация данных как конфиденциальных осуществляется в индивидуальном порядке, так как в разных странах конфиденциальной могут считать различную информацию. Тем не менее существует предположение о том, что данные, связанные с расовой или этнической принадлежностью, политическими взглядами, религиозными / философскими убеждениями, принадлежностью к вооруженным группам, сексуальной жизнью или сексуальной ориентацией, относятся к категории конфиденциальных. Презумпция конфиденциальности также применяется к персональным данным, связанным с участием субъекта данных в каком-либо правовом процессе (например, дача показаний, получение по-

вестки в суд, участие в допросе, расследование, арест, судебный процесс или вынесение приговора), к персональным данным, связанным с мерами в области безопасности в отношении субъекта данных (включая наблюдение, ограничение свободы передвижения и лишение свободы), а также к персональным данным, связанным с внутренними расследованиями или дисциплинарными мерами в МККК. Биометрические данные, генетическая информация и информация о состоянии здоровья считаются конфиденциальными во всех странах и регионах.

Нарушение безопасности данных — нарушение безопасности, которое ведет к случайному или противозаконному уничтожению, потере или изменению передаваемых, хранящихся или иным образом обрабатываемых персональных данных или к неправомерному раскрытию таких данных либо получению доступа к ним.

Независимая контрольная комиссия МККК по защите данных (Комиссия МККК по защите данных) — независимый орган, отвечающий за выполнение задач, определенных соответствующими правилами МККК по защите персональных данных, и имеющий необходимые полномочия для этого, в частности, отвечающий за наличие эффективных и реализуемых прав субъектов данных и эффективных и независимых средств правовой защиты.

Обработка — любая операция или набор операций, выполняемых с персональными данными или наборами персональных данных как автоматическими, так и иными средствами, такие как сбор, запись, организация, структурирование, хранение, адаптирование или изменение, извлечение, обращение к данным, использование, раскрытие посредством передачи, распространения или предоставления иного доступа, группировка или комбинирование либо удаление.

Обработчик — лицо, государственный орган, учреждение или иной орган, который осуществляет обработку персональных данных в интересах контролера МККК.

Ответственное лицо МККК — сотрудник МККК в каждой структуре на местах и в отделах штаб-квартиры, который уполномочен контролером МККК осуществлять руководство в определенной области деятельности в рамках мандата МККК. Сюда входят координаторы по вопросам предоставления защиты, координаторы по вопросам оказания помощи, координаторы по связям с общественностью, координаторы по вопросам

сотрудничества, координаторы по административным вопросам и, там где они присутствуют, координаторы по вопросам экономической безопасности, координаторы по вопросам водоснабжения и улучшения условий проживания, координаторы по вопросам здравоохранения, координаторы по вопросам судебной медицины, а также руководящий персонал МККК. В штаб-квартире МККК ответственные лица МККК — это руководители подразделений или сотрудники, которым они делегировали полномочия по выполнению функций ответственных лиц МККК.

Передача данных — все действия, в результате которых у третьих сторон за пределами МККК появляется доступ к персональным данным, будь то на бумаге, электронных носителях, через интернет или посредством любого другого метода.

Персональные данные — любая информация, относящаяся к идентифицированному или идентифицируемому физическому лицу. Она может включать в себя такие идентификаторы, как ФИО или аудиовизуальные материалы, идентификационный номер, данные о местонахождении или идентификатор подключения к сети; сюда также может относиться информация, связанная с физическими, физиологическими, генетическими, психологическими, экономическими, культурными или социальными характеристиками субъекта данных. Этот термин также включает в себя информацию, с помощью которой осуществляется или становится возможным установление принадлежности человеческих останков.

Для определения того, можно ли идентифицировать человека, должны приниматься во внимание все средства, которые с разумной долей вероятности могут использоваться контролером или иным лицом для осуществления идентификации прямым или косвенным образом. Чтобы определить, какие средства с разумной долей вероятности будут использоваться для идентификации лица, необходимо принять во внимание все объективные факторы, такие как расходы на идентификацию и необходимое для этого время, с учетом технологий, доступных на момент обработки данных, и технических достижений. Таким образом, персональные данные не включают в себя анонимную информацию, то есть информацию, которая не относится к идентифицированному или идентифицируемому физическому лицу, или данные, которые были анонимизированы таким образом, что идентифицировать субъекта данных невозможно (перестало быть возможным). Поэтому правила МККК по защите персональных данных не распространяются на обра-

ботку такой анонимной информации, в том числе осуществляемую для сбора статистики или в исследовательских целях.

Лица, пользующиеся сетевыми сервисами, могут быть ассоциированы с идентификаторами подключения к сети, которые предоставляются их устройствами, приложениями, инструментами и протоколами (такими как адреса интернет-протоколов или идентификаторы файлов cookie) и являются персональными данными. Такое использование сетевых сервисов может оставлять следы, которые — вместе с уникальными идентификаторами и иной информацией, получаемой серверами, — могут быть использованы для составления профиля лица и его идентификации.

Получатель — лицо, государственный орган, учреждение или иной орган, который получает переданные данные.

Представитель по вопросам защиты данных — сотрудник МККК в каждой делегации МККК или в каждом отделе штаб-квартиры МККК, назначенный для обеспечения применения настоящих правил и механизмов, предусмотренных в них.

Профилирование — любая форма автоматизированной обработки персональных данных, в том числе с использованием систем машинного обучения. Профилирование заключается в использовании персональных данных для оценки некоторых аспектов личности человека, в частности для анализа или прогнозирования эффективности его работы, финансового положения, состояния здоровья, личных предпочтений, интересов, надежности, поведения, местонахождения или передвижений.

Согласие — любое свободно данное конкретное и сознательное указание о своей воле, которым субъект данных оповещает о своем согласии на обработку касающихся его персональных данных.

Субъект данных — физическое лицо (человек), личность которого можно установить (идентифицировать) прямым или косвенным образом, в частности на основании персональных данных.

МККК помогает людям, пострадавшим от вооруженных конфликтов и других ситуаций насилия по всему миру. Организация делает все возможное, чтобы защитить их жизнь и достоинство и облегчить их страдания. В этой работе МККК часто сотрудничает со своими партнерами по Движению Красного Креста и Красного Полумесяца. Настаивая на соблюдении гуманитарного права и продвигая универсальные гуманитарные принципы, организация стремится предотвратить страдания людей.

www.icrc.org/ru
t.me/mkkk_ru
vk.com/icrc_rus

Международный Комитет Красного Креста
19 avenue de la Paix
1202, Женева, Швейцария
T +41 22 734 60 01
shop.icrc.org

МККК

4261/005 03.2026