РЕКОМЕНДАЦИЯ № REC (2010) 13
КОМИТЕТА МИНИСТРОВ СТРАНАМ-ЧЛЕНАМ СОВЕТА ЕВРОПЫ ПО ВОПРОСАМ ЗАЩИТЫ ЧАСТНЫХ ЛИЦ В СВЯЗИ С АВТОМАТИЗИРОВАННОЙ ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ В КОНТЕКСТЕ ПРОФИЛИРОВАНИЯ

Утверждена Комитетом Министров 23 ноября 2010 года

Комитет министров,

исходя из того, что целью Совета Европы является достижение все большего единства между его членами;

отмечая, что информационные и коммуникационные технологии (ИКТ) делают возможными сбор и обработку больших объёмов данных, включая персональные данные, как в частном, так и в общественном секторах; отмечая, что данные ИКТ используются в большом диапазоне различных целей, в том числе для использования услуг, общепринятых и ценных для общества, потребителей и экономики; отмечая в то же время, что беспрерывное развитие конвергентных технологий создает для общества новые вызовы в связи со сбором и дальнейшей обработкой данных;

отмечая, что такие сбор и обработка информации могут проводиться в различных ситуациях и для достижения различных целей, и касаются различных видов данных, таких как информационные потоки, запросы пользователей Интернета, привычки потребителя, их деятельность, образ жизни и поведение пользователей телекоммуникационных устройств, в том числе данные о месте (местах) их нахождения, а также данные, получаемые, в частности, из социальных сетей, систем видеонаблюдения, биометрических систем и радиочастотной идентификации (РЧИД), предвестников “Интернета вещей”, а также, отмечая желательность оценки различных ситуаций и целей в дифференцированной и многообразной форме;

отмечая, что данные, собранные таким способом, обрабатываются на основе соответствующих расчётов, сравнений и программ статистической корреляции, с целью подготовки профилей граждан, которые могут быть использованы многочисленными и разнообразными способами, путём сопоставления данных нескольких лиц; отмечая, также, что дальнейшее развитие ИКТ позволяет осуществлять указанные операции за относительно низкую плату;

исходя из того, что в результате этого установления связей между большим количеством персональных, пусть даже анонимных заключений, метод профилирования граждан может отразиться на соответствующих людях, поскольку они попадают в определенные категории, причем зачастую об этом не зная;

исходя из того, что профильные характеристики, когда они присваиваются субъекту данных, делают возможным создание новых персональных данных, которые не являются идентичными тем, которые были переданы указанным субъектом контролёру или которые известны контролёру, как могли обоснованно полагать лица передающие эти данные;

исходя из того, что недостаточная прозрачность или даже просто «невидимость» профилирования граждан и отсутствие точности, которая может проистекать из автоматического применения заранее установленных правил для выводов, может создавать значительный риск для прав и свобод человека;

исходя, в частности, из того, что защита основных прав человека, и в первую очередь права на частную жизнь и защиту персональных данных, обеспечивается наличием различных независимых сфер частной жизни, в которых каждый человек имеет право контролировать использование того, что она или он считают составляющей их идентичность;

исходя из того, что профилирование граждан может отвечать законным интересам как лица, которое его использует, так и лица, к которому такие данные относятся, например,

когда это приводит к более высокому уровню рыночной сегментации, обеспечивает анализ рисков или мошенничества или адаптирует предложения для удовлетворения потребительского спроса путём оказания более совершенных услуг; а также исходя из того, что указанное профилирование может принести определенные преимущества пользователям, экономике и обществу в целом;

полагая, однако, что, профилирование отдельного лица может привести к неоправданному лишению её/его права доступа к тем или иным товарам или услугам, тем самым нарушая принцип недопустимости дискриминации;

полагая, кроме того, что методы профилирования, выявляя взаимосвязи между конфиденциальными данными в смысле статьи 6 Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СЕД № 108, ниже именуемая "Конвенция № 108") и других данных, может привести к созданию новых чувствительных данных, касающихся идентифицированного или неидентифицируемого лица; а, также учитывая, что такое профилирование может подвергнуть людей весьма значительным рискам дискриминации и посягательства на их личные права и достоинство;

исходя из того, что профилирование детей могут иметь серьёзные последствия для всей их последующей жизни, с учётом их неспособности от своего имени давать своё свободное, конкретное и информированное согласие при сборе личных данных для профилирования, и поэтому необходимо принимать конкретные и надлежащие меры для защиты детей, с учетом высших интересов ребёнка и развития его личности в соответствии с Конвенцией ООН о правах ребёнка;

исходя из того, что использование профилей граждан, пусть даже и законным путём, без необходимых предосторожностей и специальных гарантий, может нанести серьезный ущерб человеческому достоинству, равно как и иным основным правам и свободам, включая экономические и социальные права;

будучи убежден в том, что необходимо регулировать процесс профилирования граждан в том, что касается защиты личных данных в целях обеспечения основных прав и свобод личности, в частности права на частную жизнь, и в целях предупреждения дискриминации по признаку пола, расы и этнического происхождения, религии или верований, инвалидности, возраста или сексуальной ориентации;

напоминая в этой связи об общих принципах защиты данных в соответствии с положениями Конвенции № 108;

напоминая о том, что каждое лицо имеет право доступа к данным, относящимся к нему или к ней лично, и полагая, что каждое лицо должно понимать логику профилирования; а также исходя из того, что данное право не должно оказывать негативного влияния на права и свободы других лиц, и в частности не должно оказывать негативного влияния на коммерческие тайны или интеллектуальную собственность или авторские права, защищающие в том числе и программное обеспечение;

напоминая о необходимости соблюдать существующие принципы, установленные другими соответствующими Рекомендациями Совета Европы, в частности, Рекомендацией Rec (2002)9 о персональных данных, собранных и обработанных в целях страхования и Рекомендацией Rec(97)18 о защите персональных данных, собранных и обработанных в целях статистики;

принимая во внимание Конвенцию Совета Европы о киберпреступности (СЕД № 185 – Будапештская Конвенция), которая содержит правила хранения, сбора и обмена данными, при соблюдении условиий и гарантий, обеспечивающих соответствующую защиту прав и свобод человека;

принимая во внимание статью 8 Европейской Конвенции по правам человека (СЕД № 5), как она толкуется Европейским судом по правам человека, а также новые риски, создаваемые в результате использования новейших информационных и коммуникационных технологий;

принимая во внимание, что защита человеческого достоинства и других основных прав и свобод человека в контексте профилирования граждан может оказаться эффективной в том случае, и только в том случае, если все заинтересованные лица и организации будут вносить совместный вклад в дело честного и законного профилирования граждан;
принимая во внимание, что мобильность людей, глобализация рынков и использование новых технологий делают необходимыми трансграничные обмены информацией, в том числе и в контексте профилирования, и требуют сравнимой степени защиты во всех государствах-членах Совета Европы,
Рекомендует правительствам государств-членов:
1. применять Приложение к данной Рекомендации о сборе и обработке персональных данных, в частности в контексте профилирования граждан, в первую очередь для принятия мер по обеспечению того, чтобы принципы, изложенные в данной Рекомендации, были отражены в их законодательстве и повседневной практике;
2. обеспечить широкое распространение принципов, установленных в указанном Приложении к данной Рекомендации, среди населения, публичных органов власти, общественных или частных органов, в особенности тех, которые участвуют в создании и использовании профилирования, таких как разработчики и поставщики программного обеспечения, разработчики профилирования, провайдеры услуг электронных коммуникаций и провайдеры услуг информационного общества, а также среди органов, отвечающих за защиту данных и стандартизацию;
3. поощрять таких лиц, публичные и частные органы вводить и поддерживать механизмы саморегулирования, такие как кодексы поведения, обеспечивающие уважение к частной жизни и защиту данных, а также внедрять технологии, упомянутые в Приложении к данной Рекомендации.

Приложение к Рекомендации CM/Rec(2010)13

1. Определения

В целях данной Рекомендации:
a. термин “персональные данные” означает любую информацию, относящуюся к идентифицированному или идентифицируемому лицу (“субъект данных») Лицо не рассматривается как “идентифицируемое”, если идентификация требует неоправданно большого времени или усилий.
b. термин “чувствительные данные” означает персональные данные, раскрывающие расовое происхождение, политические взгляды, религиозные и иные верования, а также данные о состоянии здоровья, сексуальной жизни или уголовных судимостях, а также другие данные, определяемые как чувствительные местным законодательством.
c. термин “обработка” означает любую операцию или комплекс операций, выполняемых полностью или частично с помощью автоматизированных процессов и применяемых к персональным данным, таких как хранение, консервация, адаптация или изменение, извлечение, ознакомление, использование, передача, подгонка или обменное соединение, в а также удаление или уничтожение.
d. термин “профиль” относится к набору данных, характеризующих категорию лиц, которые направлены на применение к какому-либо лицу.
e. термин “профилирование” означает метод и приёмы автоматизированной обработки, состоящей из применения “профиля” к какому-либо лицу с целью принятия решения, касающиеся её или его или же для анализа или прогноза её или его личных предпочтений, поведения и позиций.
f. термин “услуги информационного общества” относится к любой услуге, обычно предоставляемой за вознаграждение на расстоянии, и осуществляемое электронным способом.
g. термин “контролёр” означает физическое или юридическое лицо, или публичный орган, агентство или любой иной орган, который самостоятельно или во взаимодействии с

другими, определяет цели и средства, используемые при сборе и обработке персональных данных.

h. термин “Обработчик” означает физическое или юридическое лицо, публичный орган, агентство или любой иной орган, которые обрабатывают персональные данные от имени контролера.

2. Общие принципы

2.1. В процессе сбора и обработки персональных данных, являющихся предметом данной Рекомендации, должно быть гарантировано уважение основных прав и свобод человека и, в первую очередь, уважение права на частную жизнь и принципа недопустимости дискриминации.

2.2. Государства-члены должны поощрять разработку и практическое внедрение процедур и систем в соответствии с принципом права на частную жизнь и защиту данных, причем уже на этапе планирования, в первую очередь на основе использования технологий, защищающих частную жизнь. Они также должны принимать надлежащие меры, направленные на противодействие развитию и использованию технологий, целиком или частично нацеленных на то, чтобы незаконными методами обойти технологические меры по защите частной жизни.

3. Условия сбора и обработки личных данных в контексте профилирования граждан

A. Соблюдение закона

3.1. Сбор и обработка персональных данных в контексте профилирования граждан должны быть добросовестными, законными и соразмерными, и предназначенными для специально оговоренных и законных целей.

3.2. Персональные данные в контексте профилирования граждан должны быть адекватными, уместными и не содержать избыточной информации с учетом целей, для которых они собираются или обрабатываются.

3.3. Персональные данные, используемые в контексте профилирования, должны храниться в форме, обеспечивающей идентификацию субъектов данных на период, не превышающий времени, необходимого для целей, в которых они были собраны и обработаны.

3.4. Сбор и обработка персональных данных в контексте профилирования может осуществляться только в случаях, если:

a. это предусмотрено законом; или

b. это разрешено законом и:

- субъект данных или её/его законный представитель имеет её/его свободное, конкретное и информированное согласие;
- это необходимо для исполнения контракта, стороной которого является субъект данных, или для применения доконтрактных мер, предпринимаемых по запросу субъекта данных;
- это необходимо для выполнения задачи, выполняемой в интересах общества или во исполнение официальных функций, возложенных на контролёра или третью сторону, которым раскрываются персональные данные;
- это необходимо для целей реализации законных интересов контролёра или третьей стороны, или сторон, которым раскрываются персональные данные, за исключением тех случаев, когда такие интересы нарушают основные права и свободы субъектов данных;
- это необходимо в жизненных интересах субъекта данных.

3.5. Сбор и обработка персональных данных в контексте профилирования лиц, которые не в состоянии от себя лично выразить свое свободное, конкретное и информированное согласие, воспрещаются, за исключением тех случаев, когда это делается в законных интересах субъекта данных или если имеется высший общественный интерес, при условии обеспечения надлежащих гарантий на основании закона.

3.6. Когда требуется такое согласие, контролёру вменяется в обязанность представить доказательства того, что субъект данных согласен, после получения соответствующей информации, на профилирование, в соответствии с положениями Раздела 4.

3.7. По мере возможности, если только требуемая услуга не требует знания субъекта данных, любой человек имеет право доступа к информации о товарах или услугах или к самим таким товарам или услугам, но без необходимости передавать свои персональные данные провайдеру таких товаров и услуг. В целях обеспечения свободного, конкретного и информированного согласия на профилирование, провайдеры услуг информационного общества должны обеспечить заочный, не профилированный доступ к информации о своих услугах.
3.8. Распространение и использование, без уведомления субъекта данных, программного обеспечения, направленного на наблюдение или мониторинг в контексте профилирования того, как используется данный терминал или электронная коммуникационная сеть, допускается только в том случае, если это конкретно предусмотрено в национальном законодательстве и сопровождается соответствующими гарантиями.

B. Качество данных

3.9. Контролёру вменяется в обязанность вносить коррективы в случаях выявления неточностей и ограничивать риски ошибок, присущих профилированию.
3.10. Контролёр должен периодически и в пределах разумного времени производить переоценку качества данных и используемых статистических выводов.

C. Чувствительные данные

3.11. Сбор и обработка чувствительных данных в контексте профилирования воспрещаются, за исключением случаев, когда такие данные необходимы для законных и конкретных целей обработки, и при условии, что национальное законодательство предусматривает соответствующие гарантии. Когда требуется согласие, то оно должно быть явно выражено, если речь идёт о чувствительных данных.

4. Информация

4.1. В тех случаях, когда личные данные собираются в контексте профилирования, контролёр должен представить субъектам данных следующую информацию:
a. что их данные будут использоваться в контексте профилирования;
b. о целях проведения профилирования;
c. о категориях персональных данных;
d. о контролёре и, при необходимости, о её/его представителе;
e. о наличии надлежащих гарантий;
f. всю информацию, необходимую для гарантий добросовестности при проведении профилирования, такую как:
- категории лиц или органов, которым могут быть переданы персональные данные, и в каких целях;
- возможность, когда это целесообразно, для субъекта данных отказать в публикации или отозвать согласие на публикацию и о последствиях отзыва;
- условия применения права доступа, возражения или поправок, а также о праве подать жалобу в компетентные органы;
- лица или органы, от которых личные данные собираются или будут собираться;
- обязательный или факультативный характер ответов на вопросы, которые будут использованы для сбора персональных данных, а также последствия для субъектов данных в случае отказа отвечать на такие вопросы;
- длительность хранения;
- предполагаемые последствия присвоения профиля субъекту данных.
4.2. В тех случаях, когда персональные данные поступают от самого субъекта данных, контролёр должен предоставить субъекту данных информацию, указанную в Принципе 4.1 не позднее времени сбора.
4.3. В тех случаях, когда персональные данные поступают не от самого субъекта данных, контролёр должен предоставить субъекту данных информацию, указанную в Принципе 4.1 как только личные данные зафиксированы или, если планируется передавать

персональные данные третьей стороне, не позднее даты первого поступления, личных данных.
4.4. В тех случаях, когда личные данные собираются без намерения применить методы профилирования и в дальнейшем обрабатываются в контексте биографических справок, контролёр должен предоставить ту же информацию, что предусмотрена в Принципе 4.1.
4.5. Положения, содержащиеся в Принципах 4.2, 4.3 и 4.4 об информировании субъекта данных, не применяются в случаях когда:
a. субъект данных уже был проинформирован;
b. доказана невозможность предоставить информацию или необходимость применения чрезмерных усилий для её сбора;
c. обработка или передача личных данных для профилирования конкретно предусматривается местным законодательством.
В случаях, упомянутых в пп. *b* и *c*, должны предусматриваться соответствующие гарантии.
4.6. Информация, предоставленная субъекту данных, должна быть надлежащей и адаптированной к обстоятельствам.

5. Права субъектов данных

5.1. Субъект данных, о котором составляется или был составлен профиль, имеет право получить от контролера, по своему запросу, в пределах разумного времени и в понятной форме, информацию, касающуюся:
a. своих персональных данных;
b. логических обоснований для обработки своих персональных данных и того, что она была использована именно для применения к ней/ему составления профиля, по крайней мере, в случае автоматизированного решения;
c. целей составления профиля и категорий лиц или организаций, которым профиль может быть передан.
5.2. Субъекты данных должны иметь право вносить коррективы, удалять или блокировать свои персональные данные, в тех случаях, когда профилирование в процессе обработки было выполнено в нарушение национального законодательства, которое обеспечивает соблюдение принципов, изложенных в данной Рекомендации.
5.3. За исключением тех случаев, когда в законодательство предусмотрено профилирование в контексте обработки личных данных, субъекты данных должны иметь право возражать, на серьезных законных основаниях, относящихся к её/его ситуации, против использования своих личных данных для профилирования. В случаях обоснованных возражений в профилировании не должны более использоваться личные данные этого субъекта данных. Если целью обработки является прямой маркетинг, то субъект данных не обязан представлять никаких обоснований.
5.4. Если имеются какие-либо основания для ограничения прав, изложенных в данном разделе, в соответствии с положениями Раздела 6, такое решение должно быть передано субъекту данных любыми средствами, пригодными для документальной регистрации, с упоминанием юридических и фактических мотивов такого ограничения.
Это упоминание может быть опущено, когда имеется причина, подвергающая опасности цель ограничения. В таких случаях субъекту данных предоставляется информация о том, как можно оспорить такое решение в компетентном национальном надзорном органе, судебной инстанции или в суде.
5.5. В тех случаях, когда лицо является субъектом решения, имеющего юридические последствия, касающиеся её/его лично, или значительно её/его затрагивающее, принятого исключительно на основании профилирования, то она или он должны иметь возможность представить свои возражения против такого решения за исключением случаев, когда:
a. это предусмотрено законом, который содержит меры по охране законных интересов субъектов данных, в частности, в частности, предоставляя им возможность изложить свою точку зрения;

b. решение было принято в процессе исполнения контракта, одной из сторон по которому является субъект данных, или во исполнение доконтрактных мер, принятых по запросу субъекта данных, и если существуют меры по обеспечению гарантий в отношении законных интересов субъектов данных.

6. Исключения и ограничения

В тех случаях, когда это необходимо в интересах демократического общества, по причинам государственной безопасности, общественного порядка, финансовых интересов государства или предотвращения и преследования уголовных преступлений или защиты интересов субъектов данных или прав и свобод других людей, странам-членам можно не применять положения Разделов 3, 4 и 5 данной Рекомендации, когда это предусмотрено законом.

7. Средства правовой защиты

Национальное законодательство должно предусматривать соответствующие санкции и средства правовой защиты в случае нарушений тех положений национального законодательства, которые обеспечивают выполнение принципов, содержащихся в данной Рекомендации.

8. Безопасность данных

8.1. Должны приниматься соответствующие меры технического и организационного характера для обеспечения защиты персональных данных, обработанных в соответствии с положениями национального законодательства, обеспечивающего соблюдение принципов, установленных данной Рекомендацией во имя охраны от случайного или незаконного уничтожения и случайной утраты, а также несанкционированного доступа, внесения изменений, передачи или любой иной формы незаконной обработки.

Такие меры должны обеспечивать надлежащий стандарт безопасности данных с учетом существующего уровня развития, а также чувствительного характера личных данных, собранных и обработанных в контексте профилирования, и оценки потенциальных рисков. Эти меры должны периодически и в разумные сроки пересматриваться.

8.2. Контролёры должны, в соответствии с национальным законодательством установить надлежащие внутренние правила с учетом принципов, изложенных в данной Рекомендации.

8.3. При необходимости, контролёры должны назначать независимых лиц, имеющих соответствующую квалификацию для консультирования по этим вопросам, которые несут ответственность за безопасность информационных систем и защиту данных.

8.4. Контролёры должны выбирать такие процессоры, которые обеспечивают адекватные гарантии в отношении технических и организационных аспектов обработки, и следят за тем, чтобы эти меры неукоснительно соблюдались и, в частности, чтобы обработка велась в соответствии с их инструкциями.

8.5. Кроме того, должны быть предусмотрены должные меры, исключающие использование таких анонимных и совокупных статистических результатов в профилировании, которые могут быть использованы для реидентификации субъектов данных.

9. Надзорные органы

9.1. Государства-члены должны дать полномочия одному или нескольким независимым органам, которые могли бы обеспечить соблюдение национального законодательства, которое реализует принципы, содержащиеся в данной Рекомендацией, и при этом такие органы должны иметь необходимые полномочия проводить расследования и вмешиваться в ситуацию, в частности полномочия рассматривать жалобы претензии любого лица.

9.2. Кроме того, в случаях обработки данных, когда используется профилирование и создаются особые риски в отношении защиты частной жизни и персональных данных, государства-члены могут предусматривать:

a. чтобы контролеры либо своевременно уведомляли надзорный орган до начала обработки, или

b. чтобы сама обработка подвергалась предварительной проверке таким надзорным органом.

9.3. Вышеупомянутые надзорные органы должны информировать общественность о применении национального законодательства, которое призвано обеспечить соблюдение принципов, изложенных в данной Рекомендации.