

**Директива Европейского Парламента и Совета Европейского Союза  
2002/58/ЕС от 12 июля 2002 г.**

**в отношении обработки персональных данных и защиты конфиденциальности в секторе  
электронных средств связи  
(Директива о конфиденциальности и электронных средствах связи)\*<sup>(1)</sup>**

**(Текст в редакции Директивы 2006/24/ЕС Европейского парламента и Совета ЕС от 15  
марта 2006 г., Директивы 2009/136/ЕС Европейского парламента и Совета ЕС от 25  
ноября 2009 г.)**

Европейский Парламент и Совет Европейского Союза,  
Руководствуясь Договором об учреждении Европейского Сообщества, и, в частности,  
Статьей 95,

принимая во внимание рекомендации Европейской Комиссии\*<sup>(2)</sup>,  
принимая во внимание заключение Европейского комитета по социальным и  
экономическим вопросам\*<sup>(3)</sup>,  
руководствуясь разъяснениями Комитета регионов,  
действуя в соответствии с процедурой, предусмотренной Статьей 251 Договора\*<sup>(4)</sup>,  
Поскольку:

(1) Директива Европейского парламента и Совета ЕС 95/46/ЕС от 24 октября 1995 г. о  
защите физических лиц при обработке персональных данных и свободном обращении таких  
данных\*<sup>(5)</sup> требует от государств-членов ЕС гарантий соблюдения прав и свобод физических  
лиц в связи с обработкой их персональных данных и в особенности их прав на  
конфиденциальность для обеспечения свободного движения потока информации о  
персональных данных в Сообществе.

(2) Настоящая Директива стремится к соблюдению основополагающих прав и  
принципов, признанных в Хартии основных прав Европейского союза. В частности, настоящая  
Директива стремится к обеспечению гарантий полного соблюдения прав, установленных  
Статьями 7 и 8 названной Хартии.

(3) Конфиденциальность коммуникаций гарантируется в соответствии с  
международными нормами, касающимися прав человека, в частности, Европейской  
Конвенцией о защите прав человека и основных свобод, а также конституциями  
государств-членов ЕС.

(4) Директива 97/66/ЕС Европейского парламента и Совета ЕС от 15 декабря 1997 г.,  
касающаяся обработки персональных данных и защиты информации о частной жизни в сфере  
телекоммуникаций\*<sup>(6)</sup> перевела принципы, установленные в Директиве 95/66/ЕС в  
специальные правила, применяемые в сфере телекоммуникаций. Директива 97/66/ЕС должна  
быть адаптирована к изменениям на рынке и в технологиях оказания услуг электронной связи  
для обеспечения равного уровня защиты персональных данных и информации о частной жизни  
пользователей общедоступных услуг электронной связи независимо от используемых  
технологий. В связи с этим указанная Директива подлежит отмене и должна быть заменена  
настоящей Директивой.

(5) В настоящее время новые передовые технологии вводятся в информационных сетях  
связи общего пользования в Сообществе, что порождает определенные требования к защите  
персональных данных и информации о частной жизни пользователя. Развитие  
информационного общества характеризуется введением новых услуг электронной связи.  
Доступ к цифровому мобильному Интернету стал возможным для широкой общественности.  
Данное средство цифровых телекоммуникаций имеет большую функциональную мощность и  
предлагает широкие возможности по обработке персональных данных. Успешное развитие этих  
услуг на международном уровне частично зависит от уверенности пользователей в том, что их  
частная жизнь будет находиться вне опасности.

(6) Интернет изменяет традиционные структуры рынка, предоставляя общую  
глобальную инфраструктуру для оказания широкого диапазона услуг электронной связи.  
Общедоступные услуги электронной связи через сеть Интернет открывают не только новые  
возможности для пользователей, но также и новые опасности, угрожающие их персональным  
данным и информации о личной жизни.

(7) Применительно к коммуникациям, осуществляемым посредством общедоступной

телекоммуникационной сети, должны быть разработаны специальные законодательные, регулятивные и технические положения, с тем чтобы обеспечить защиту основных прав и свобод физических лиц и законных интересов юридических лиц. В особенности это имеет большое значение в связи с увеличивающейся способностью автоматизированного хранения и обработки персональных данных абонентов и пользователей.

(8) Законодательные, регламентарные и административные положения, принятые государствами-членами ЕС в отношении защиты персональных данных, информации о частной жизни и законных интересов юридических лиц в сфере электронных коммуникаций, должны быть согласованы, с тем чтобы избежать препятствий на внутреннем рынке услуг электронной связи в соответствии со Статьей 14 Договора. Такое согласование должно быть сведено к установлению требований, необходимых для гарантии того, что продвижение и развитие новых услуг связи в сфере электронных коммуникаций и информационных сетей между государствами-членами ЕС не имеют препятствий.

(9) Государства-члены ЕС как провайдеры и пользователи совместно с компетентными органами Сообщества, должны сотрудничать в вопросах введения и развития соответствующих технологий, если это необходимо для обеспечения гарантий, предусмотренных настоящей Директивой, при этом принимая в особый расчет цели минимизации обработки персональных данных и использования по возможности анонимных данных или данных, представленных под псевдонимом.

(10) В сфере электронных коммуникаций Директива 95/46/ЕС применяется, в частности, в отношении всех случаев, касающихся защиты основных прав и свобод, которые специально не затрагиваются настоящей Директивой, включая обязательства оператора и права индивидов. Директива 95/46/ЕС применяется в отношении не публичных услуг предоставления связи.

(11) Так же, как и Директива 95/46/ЕС, настоящая Директива не обращается к проблемам защиты основных прав и свобод, связанных с осуществлением видов деятельности, не регулируемых законодательством Сообщества. Поэтому она не изменяет существующий баланс между правом индивида на частную жизнь и возможностью государств-членов ЕС принять меры, упомянутые в Статье 15(1) настоящей Директивы, необходимые для защиты общественной безопасности, обороны, государственной безопасности (включая экономическое благосостояние государства, когда деятельность имеет отношение к делам государственной безопасности) и применение уголовного права. Следовательно, настоящая Директива не оказывает влияния на способность государств-членов ЕС производить законный перехват информации, передаваемой с помощью электронной связи, или принимать другие необходимые меры для любой из этих целей, в соответствии с Европейской конвенцией о защите прав человека и основных свобод, и разъяснениями, содержащимися в постановлениях Европейского суда по правам человека. Такие меры должны быть уместными, строго пропорциональными намеченной цели и необходимыми в пределах демократического общества и должны относиться к адекватным мерам безопасности в соответствии с Европейской конвенцией о защите прав человека и основных свобод.

(12) Абонентами общедоступных услуг электронной связи могут являться физические или юридические лица. В дополнение к Директиве 95/46/ЕС настоящая Директива имеет целью защиту основных прав физических лиц и, в частности, их права на частную жизнь так же, как и законных интересов юридических лиц. Настоящая Директива не влечет за собой обязательств государств-членов ЕС по расширению сферы применения Директивы 95/46/ЕС для защиты законных интересов юридических лиц, применяемой в рамках действующего законодательства Сообщества и национального законодательства.

(13) Договорное отношение между абонентом и провайдером может повлечь за собой осуществление абонентом периодических платежей или единовременной платы за оказанные услуги или услуги, подлежащей оказанию. Заранее оплаченные карты также рассматриваются в качестве договора.

(14) Местонахождение данных может характеризоваться широтой, долготой и высотой терминального оборудования пользователя, направлением пути, уровнем точности информации о размещении данных, идентификацией ячейки сети, в которой располагается терминальное оборудование пользователя в определенный момент времени, и временем регистрации информации о размещении данных.

(15) Коммуникация может включать любое обозначение, перечисление или адресацию информации, предоставленной отправителем сообщения или пользователем связи для

осуществления коммуникации. Трафик данных может включать любое перемещение информации через сеть, по которой осуществляется коммуникация с целью передачи данных. Трафик данных, *inter alia*, включает сведения о направлении, длительности, времени передачи или объеме передаваемого сообщения, используемом протоколе, месте положения терминального оборудования отправителя или получателя сообщения, сети, по которой начинается или заканчивается соединение, начале, конце, продолжительности соединения. Эти данные также могут включать информацию о формате, в котором передается сообщение по сети передачи данных.

(16) Информация, являющаяся частью теле-радиовещательных услуг, предоставляемая через сеть связи общего пользования, предназначается для потенциально неограниченного круга лиц и не относится к коммуникациям в значении настоящей Директивы. Однако в случаях, когда индивидуальный пользователь или абонент, получающий такую информацию, может быть идентифицирован, например, при помощи услуги предоставления видеоканала по требованию, передаваемая информация охватывается понятием коммуникации, применяемым для целей настоящей Директивы.

(17) Для целей настоящей Директивы согласие пользователя или абонента, независимо от того, является последний юридическим или физическим лицом, должно иметь то же значение, что и согласие в отношении данных, определяемое и описываемое далее в Директиве 95/46/ЕС. Согласие может быть дано любым соответствующим способом, позволяющим установить свободно выраженное и осознанное волеизъявление пользователя, в том числе с помощью проставления отметки при посещении Интернет-сайта.

(18) Дополнительные услуги могут, к примеру, включать консультации по выбору наименее дорогих тарифных планов, руководства по выбору маршрутов, транспортную информацию, прогнозы погоды и информацию для туристов.

(19) Предъявление определенных требований, относящихся к презентации и блокированию вызывающего и идентифицированного соединенного номера и автоматическому повтору вызова абонентского номера, связанного с моделирующим устройством, не должно производиться в обязательном порядке в случаях, когда выполнение таких требований окажется технически невозможным или потребует осуществления непропорциональных экономических затрат. Для заинтересованных сторон важно быть информированными о таких случаях, поэтому государствам-членам ЕС следует уведомлять о них Европейскую Комиссию.

(20) Операторы должны принять соответствующие меры для обеспечения безопасности предоставляемых услуг, если это необходимо, то совместно с провайдером сети, и информировать абонентов о любых экстренных угрозах повреждения безопасности сети. Возможность наступления такой угрозы особенно характерна для услуг электронных коммуникаций, предоставляемых в открытой сети, такой как Интернет или в аналогичной ей мобильной телефонной сети. Абонентам и пользователям таких услуг особенно важно быть полностью информированными своими провайдерами о существующих угрозах повреждения безопасности, выходящих за пределы средств защиты, имеющихся у провайдера. Провайдеры, предоставляющие услуги коллективного доступа в сеть Интернет, должны информировать пользователей и абонентов о мерах, которые они могут предпринять для защиты безопасности их коммуникаций, например, с помощью использования специального программного обеспечения или технологий шифрования. Требование об информировании абонентов о возможных угрозах безопасности не освобождает провайдера от обязанности предпринять за свой счет соответствующие неотложные меры для нейтрализации любых новых непредвиденных угроз безопасности и восстановить нормальный уровень безопасности коммуникаций. Предоставление абоненту информации об угрозе безопасности должно быть бесплатным, за исключением той номинальной платы, которую осуществляет абонент при получении или сборе информации, например, при скачивании сообщения, отправленного по электронной почте. Безопасность оценивается в свете Статьи 17 Директивы 95/46/ЕС.

(21) Для того чтобы защитить конфиденциальность коммуникаций, включая их содержание и любые данные, имеющие отношение к этим коммуникациям, должны быть предприняты меры по предотвращению несанкционированного доступа к таким коммуникациям посредством сетей связи общего пользования и общедоступных услуг электронной связи. Национальным законодательством отдельных государств-членов ЕС запрещается только международный несанкционированный доступ к коммуникациям.

(22) Запрещение хранения сообщений и относящихся к ним данных о трафике лицам, не

являющимся пользователями, или без согласия пользователей не подразумевает запрет любого автоматического, промежуточного и временного хранения данной информации, необходимого исключительно в целях ее передачи по сети электронной связи. При этом предусматривается, что информация не хранится дольше, чем это необходимо для ее передачи и управления трафиком, и что в течение такого периода хранения гарантируется ее конфиденциальность. Настоящая Директива не должна препятствовать более длительному хранению такой информации при наличии необходимости оптимизации дальнейшей передачи общедоступной информации пользователям услуги по их запросу, учитывая, что эта информация будет в любом случае находиться в общем доступе без ограничения, и что любые данные об индивидуальных пользователях или абонентах, запрашивающих такую информацию, уничтожаются.

(23) Конфиденциальность коммуникаций должна также быть гарантирована в законной деловой практике. В случае, когда это необходимо и разрешено законодательно, сообщения могут быть записаны в целях предоставления доказательств совершения коммерческих сделок. Директива 95/46/ЕС предусматривает такую обработку данных. Стороны, обменивающиеся сообщениями, должны быть заранее осведомлены о том, что информация записывается, о целях записи информации и о длительности хранения информации. Сохраненное сообщение должно быть удалено, как только это будет возможным, но в любом случае не позднее окончания срока, в течение которого сделка может быть оспорена по закону.

(24) Терминальное оборудование пользователей сетей электронной связи и любая информация, хранящаяся на таком оборудовании, относятся к сфере частной жизни пользователей, требующей защиты в соответствии с Европейской конвенцией о защите прав человека и основных свобод. Так называемые шпионские программы, компьютерные вирусы, скрытые идентификаторы и другие аналогичные устройства могут внедряться на терминальное оборудование пользователей без их ведома с целями получения доступа к информации, хранения скрытой информации или отслеживания деятельности пользователя и могут серьезным образом вторгнуться в личную жизнь этих пользователей. Использование подобных программ может быть разрешено только в законных целях с уведомлением пользователей, которых это касается.

(25) Тем не менее, подобные программы, например, так называемые "cookies"\*(7) могут быть законным и полезным инструментом, к примеру, в анализе эффективности проекта веб-сайта и его рекламирования, а также для подтверждения соответствия пользователей, совершающих сделки он-лайн. В случаях, когда указанные программы, например cookies, предназначаются для законной цели, такой как содействие оказанию информационных общественных услуг, их использование должно быть разрешено с условием, что пользователи обеспечиваются ясной и точной информацией в соответствии с Директивой 95/46/ЕС о целях cookies или аналогичных программ для гарантии того, что пользователи осознают информацию, помещенную на используемое ими терминальное оборудование. Пользователи должны иметь возможность отказаться от cookies или другой аналогичной программы, сохраненных на их терминальном оборудовании. Это особенно важно, когда кроме основного пользователя к его терминальному оборудованию имеют доступ другие пользователи, получающие тем самым доступ к личным сведениям, хранящимся на таком оборудовании. Предупреждение о сохранении программ на терминальном оборудовании пользователя и информирование пользователя о возможности отказа от такого сохранения может быть сделано однажды перед использованием различных программ, подлежащих установке на терминальном оборудовании пользователя в течение одного соединения, а также может распространяться на любое дальнейшее использование этих программ в течение последующих соединений. Предупреждение о сохранении программ на терминальном оборудовании пользователя и информирование пользователя о возможности отказа от такого сохранения, а также запрос согласия пользователя должны осуществляться максимально удобными для пользователя способами. Доступ к определенному содержанию веб-сайта все еще может ставиться в зависимость от того, насколько хорошо cookies или аналогичное устройство, используемое в законных целях, осуществляет информационное распознавание.

(26) Данные об абонентах, обработанные в сетях электронной связи для установления соединения и передачи информации, содержат сведения о частной жизни физических лиц и касаются их прав на уважительное отношение к переписке либо затрагивают законные интересы юридических лиц. Такие данные могут храниться в пределах ограниченного срока, в течение того времени, которое необходимо для автоматизированного формирования счетов за

пользование связью (биллинга) и за межсоединение. Любая дальнейшая обработка таких данных, которую может произвести провайдер общедоступных услуг электронной связи для продвижения услуг электронной связи или для оказания дополнительных услуг, может быть осуществлена только с согласия абонента, полученного на основе точной и полной информации, предоставленной провайдером общедоступных услуг электронной связи. Данная информация должна содержать сведения о видах дальнейшей обработки данных, которые собираются произвести провайдер и о праве абонента не давать согласие или аннулировать свое согласие на такую обработку. Данные трафика, использованные для продвижения услуг связи или для оказания дополнительных услуг также должны быть удалены или сделаны анонимными после оказания услуги. Провайдеры должны всегда держать абонентов в курсе того, какие виды данных они обрабатывают, с какими целями и в течение какого периода времени.

(27) Точный момент завершения передачи сообщения, после которого данные трафика подлежат удалению, за исключением целей биллинга, может зависеть от вида предоставляемых услуг электронных коммуникаций. Например, при телефонном звонке передача голосового сообщения будет завершена в тот момент, когда любой из пользователей прекратит соединение. При использовании электронной почты передача сообщения заканчивается в тот момент, когда адресат получает сообщение, как правило, от сервера своего провайдера.

(28) Обязательство удалить данные трафика или сделать такие данные анонимными после того, как в них исчезает необходимость для передачи сообщения, не противоречит таким процедурам в Интернет, как кэширование в доменной именной системе IP адресов или кэширование IP адресов, привязанных к физическим адресам или использование информации о логине для управления правом доступа к сетям или услугам.

(29) Провайдер услуг при необходимости в индивидуальных случаях может обрабатывать данные трафика, имеющие отношение к абонентам и пользователям, для обнаружения технического отказа или ошибки в передаче сообщений. Данные трафика, необходимые для биллинга, также могут быть обработаны провайдером для обнаружения и пресечения мошенничества, заключающегося в неоплаченном пользовании услугами электронной связи.

(30) Системы предоставления услуг пользования сетями электронной связи должны быть разработаны так, чтобы ограничить количество необходимых персональных данных до строгого минимума. Любые виды деятельности, относящиеся к услугам электронной связи, но не связанные с передачей сообщений и биллингом, должны основываться на обобщенных данных трафика, которые не могут относиться к абонентам и пользователям. В случае, когда такие виды деятельности не могут быть основаны на обобщенных данных, их следует рассматривать как дополнительные услуги, для которых требуется согласие абонента.

(31) Необходимость получения согласия пользователя или абонента на обработку персональных данных в целях оказания отдельной дополнительной услуги будет зависеть от данных, подлежащих обработке, и от вида услуги, подлежащей оказанию, а также от того, будет ли возможно технически, процедурно и в договорном порядке различить, каким абонентом осуществляется индивидуальное пользование услугой электронной связи: физическим или юридическим лицом.

(32) В случае, когда провайдер услуг электронной связи или дополнительных услуг заключает с другим юридическим лицом агентский договор по обработке персональных данных, необходимых для предоставления этих услуг, такой договор и последующая обработка данных должны быть в полном соответствии с требованиями, предъявляемыми к операторам и обработчикам по обработке персональных данных, установленными в Директиве 95/46/ЕС. В случае, когда предоставление дополнительных услуг требует направления данных трафика или данных местоположения провайдером услуг электронной связи провайдеру дополнительных услуг, абоненты или пользователи, к которым относятся эти данные, должны быть также полностью информированы о совершении такой отправки перед тем, как дать свое согласие на обработку данных.

(33) Введение перечисленных биллинговых счетов улучшило положение абонентов, предоставив им возможность проверять точность снимаемых провайдером сумм. В то же время данное нововведение способно подвергнуть угрозе безопасность информации о частной жизни пользователей общедоступных услуг электронной связи. Поэтому для защиты информации о частной жизни пользователей государствам-членам ЕС следует поощрять развитие таких опций

услуг электронной связи, как альтернативные системы оплаты, позволяющие осуществлять анонимный или строго частный доступ к общедоступным услугам электронной связи, например, с помощью телефонных карт или оплату с помощью кредитных карт. К тому же государства-члены ЕС могут просить операторов предлагать своим абонентам другой вид детализированного счета, в котором определенное количество цифр вызываемого номера было удалено.

(34) Что касается идентификации вызывающего номера, то здесь необходимо защитить право вызывающей стороны скрывать показ номера, с которого осуществляется вызов, а также право принимающей стороны отклонять вызовы с неопределенных номеров. В определенных случаях существует обоснование для отмены устранения показа номера, с которого осуществляется вызов. Определенные абоненты, в частности, телефонные линии помощи и подобные организации, заинтересованы в гарантировании анонимности вызывающих их абонентов. Что касается соединенного номера, то здесь необходимо защитить право и законный интерес вызываемой стороны отказать в показе идентифицированного номера, с которым вызывающая сторона уже соединена, в особенности в случае последующих вызовов. Провайдеры общедоступных услуг электронной связи должны информировать своих абонентов о наличии в сети идентификации вызывающего и соединенного номера и обо всех услугах, предлагаемых на базе идентификации вызывающего и соединенного номера, так же как и о доступных частных опциях. Это позволит абонентам сделать выбор, основанный на знаниях о частных опциях, которые они могут использовать. Частные опции, предлагаемые для каждого телефонного номера, не обязательно должны быть доступны в качестве автоматической услуги сети, но могут быть получены по простому запросу, направленному провайдеру общедоступных услуг электронной связи.

(35) В цифровых мобильных сетях данные о географическом местоположении терминального оборудования пользователя услуг мобильной связи обрабатываются для того, чтобы сделать возможной передачу сообщений. Такие данные являются данными трафика, подпадающими под действие Статьи 6 настоящей Директивы. Однако, в дополнение, цифровые мобильные сети могут располагать возможностью по обработке данных местоположения, более точных, чем это необходимо для передачи сообщений, и используемых для предоставления дополнительных услуг, таких как индивидуализированная информация о трафике или путевой навигатор для водителей. Обработка данных, необходимых для оказания дополнительных услуг, может допускаться только после получения согласия абонентов на такую обработку. Даже в случаях, когда абоненты дали свое согласие, они должны иметь возможность бесплатно и простым способом изъять временный отказ от обработки данных местоположения.

(36) Государства-члены ЕС могут ограничить права пользователей и абонентов на частную жизнь в отношении определения номера вызывающего абонента, в случаях, когда это необходимо для отслеживания злонамеренных вызовов, а также в отношении определения номера вызывающего абонента и данных местоположения, когда это необходимо в целях наиболее эффективного выполнения своих задач службами скорой помощи. Государства-члены ЕС могут принять специальные положения для того, чтобы уполномочить провайдеров услуг электронной связи обеспечивать доступ к определению номера вызывающего абонента и данным местоположения без предварительного согласия заинтересованных абонентов или пользователей.

(37) Абонентам должны быть предоставлены гарантии от помех, которые могут быть вызваны автоматическим повтором вызова другими лицами. Более того, в таких случаях абонентам должна быть предоставлена возможность остановить повторные вызовы, посылаемые на их оборудование, простым запросом, направленным провайдеру общедоступных услуг электронной связи.

(38) Справочники абонентов услуг электронной связи широко распространены и общедоступны. Право на частную жизнь физических лиц и законные интересы юридических лиц требуют предоставления абонентам возможности определить, опубликованы ли их личные данные в справочнике, и если да, то какие именно. Поставщики общедоступных справочников должны информировать абонентов, подлежащих включению в справочник, о целях, которые преследует справочник и о любом возможном способе использования электронной версии общедоступного справочника, особенно о таких функциях поиска, встроенных в программное обеспечение, как обратный поиск, позволяющий пользователям справочника находить имя и адрес абонента на основе одного телефонного номера.

(39) Обязательство информировать абонентов о целях общедоступных справочников, в которые подлежат включению личные данные абонентов, возлагается на сторону, собирающую данные для такого включения. В случаях, когда данные могут быть переданы одному или более третьим лицам, абонент должен быть информирован о такой возможности и о получателях или категориях возможных получателей. Любая передача данных возможна при условии, что данные не могут быть использованы для целей иных, чем те, для которых они были собраны. Если сторона, осуществляющая сбор данных у абонента, или любая третья сторона, в адрес которой были переданы данные, желает использовать данные для какой-либо дополнительной цели, то новое согласие абонента должно быть получено либо инициативной стороной по сбору данных, либо третьей стороной, в адрес которой были переданы данные.

(40) Абонентам должны быть предоставлены гарантии от невмешательства в их частную жизнь незапрашиваемых сообщений, посылаемых в целях прямого маркетинга с помощью устройств автоматического вызова, телефаксов, электронных писем, в том числе SMS сообщений. Эти формы незапрашиваемых коммерческих сообщений с одной стороны относительно просты и дешевы для отправки, но с другой стороны могут наложить бремя оплаты на получателя. Более того, в некоторых случаях их объем может создать трудности для сетей электронной связи и терминального оборудования. Для таких форм незапрашиваемых сообщений, посылаемых в целях прямого маркетинга, оправдано требовать того, чтобы перед отправкой таких сообщений было получено явное согласие получателей. Единый рынок требует согласованного подхода для обеспечения простых общих правил Сообщества для организаций и пользователей.

(41) В контексте существующих клиентских отношений будет разумным допустить использование данных электронного контакта для предложения аналогичных товаров и услуг, но только той компанией, которая получила данные электронного контакта в соответствии с Директивой 95/46/ЕС. После того, как получены данные электронного контакта, клиент должен быть информирован об их дальнейшем использовании в целях прямого маркетинга ясным и отчетливым образом, а также должен получить возможность изъять отказ от такого использования данных. Уведомление о возможности отказа должно осуществляться бесплатно при каждом последующем сообщении, посылаемом в целях прямого маркетинга, за исключением платы, взимаемой за передачу сообщения, содержащего отказ.

(42) Другие формы прямого маркетинга, которые являются более дорогостоящими для отправителя и не налагают никаких финансовых затрат на абонентов и пользователей, такие как голосовые телефонные звонки одного лица другому, могут оправдывать поддержание системы, дающей абонентам или пользователям возможность показывать, что они не хотят получать такие звонки. Однако для того чтобы не уменьшать существующие уровни защиты информации о частной жизни, государства-члены ЕС должны наделяться правом поддерживать национальные системы, позволяя осуществлять такие звонки только в отношении тех абонентов и пользователей, которые дали свое предварительное согласие.

(43) В целях обеспечения эффективной реализации правил Сообщества в отношении незапрашиваемых сообщений в целях прямого маркетинга необходимо запретить использование ложных идентификаторов или ложных адресов возврата или номеров во время отправки незапрашиваемых сообщений в целях прямого маркетинга.

(44) Отдельные системы электронной почты позволяют абонентам просматривать отправителя и предметную линию электронной почты, а также удалять сообщение без необходимости загрузки остального содержания электронного сообщения и любых прикрепленных файлов, снижая таким образом затраты, которые могут возникнуть в результате загрузки незапрашиваемых электронных сообщений или прикрепленных файлов. Данные меры могут продолжать оставаться полезными в отдельных случаях как дополнительное средство к основным обязательствам, установленным в настоящей Директиве.

(45) Настоящая Директива не противоречит мерам, принимаемым государствами-членами ЕС для защиты законных интересов юридических лиц в отношении незапрашиваемых сообщений, отправляемых в целях прямого маркетинга. В случаях когда государства-члены ЕС устанавливают для юридических лиц, являющихся в основном деловыми пользователями, реестр, свободный от получения незапрашиваемых сообщений, полностью применяются положения Статьи 7 Директивы 2000/31/ЕС Европейского парламента и Совета ЕС от 8 июня 2000 г. о некоторых правовых аспектах услуг информационного общества и, в частности, об электронной торговле на внутреннем рынке (Директива об электронной

торговле\*(8)).

(46) Функциональные возможности для оказания услуг электронной связи могут быть интегрированы в сети или в любой части терминального оборудования пользователя, включая программное обеспечение. Защита персональных данных и информации о частной жизни пользователя общедоступных услуг электронной связи должна быть независимой от конфигурации различных компонентов, необходимых для оказания услуги и от распределения необходимых функциональных возможностей между этими компонентами. Директива 95/46/ЕС охватывает любую форму обработки персональных данных независимо от используемой технологии. Существование особых правил оказания услуг электронной связи наряду с общими правилами для других компонентов, необходимых для оказания таких услуг, не может способствовать защите персональных данных и информации о частной жизни технологически нейтральным способом. В связи с этим представляется необходимым принятие мер, требующих от производителей отдельных видов оборудования, используемого для оказания услуг электронной связи, создавать их программный продукт таким образом, чтобы он содержал гарантии того, что персональные данные и информация о частной жизни абонентов и пользователей защищены должным образом. Принятие таких мер в соответствии с Директивой 1999/5/ЕС Европейского парламента и Совета ЕС от 9 марта 1999 г. о радиооборудовании и телекоммуникационном терминальном оборудовании и взаимном признании их соответствия\*(9) будет гарантировать, что внедрение технических особенностей оборудования для оказания услуг электронной связи, включая программное обеспечение для защиты данных, согласовано таким образом, чтобы соответствовать потребностям обеспечения внутреннего рынка.

(47) В случае если произошло несоблюдение прав пользователей и абонентов, национальное законодательство должно предусматривать судебные средства защиты. Штрафы должны быть наложены на любое лицо, независимо от того какое право на него распространяется: частное или публичное, если данное лицо не в состоянии выполнить меры, принятые в соответствии с настоящей Директивой.

(48) В сфере применения настоящей Директивы будет полезным заимствование опыта Рабочая группа по защите личности в связи с обработкой персональных данных, созданной в соответствии со Статьей 29 Директивы 95/46/ЕС, и состоящей из представителей контрольных органов государств-членов ЕС.

(49) В целях обеспечения соответствия с положениями настоящей Директивы, необходимо предпринять отдельные специальные меры по обработке данных, выполнимые уже на дату вступления в силу национального законодательства, вводящего в действие нормативные акты, принятые согласно настоящей Директиве, приняли настоящую Директиву:

## **Статья 1**

### **Цели и область применения**

1. Настоящая Директива обеспечивает гармонизацию национальных положений, необходимых для гарантии соответствующего уровня защиты основных прав и свобод, и, в частности, права на частную жизнь и конфиденциальность информации о частной жизни в связи с обработкой персональных данных в сфере электронных коммуникаций, и для обеспечения свободного движения таких данных, передвижения оборудования для электронной связи и услуг электронной связи в Сообществе.

2. Положения настоящей Директивы конкретизируют и дополняют Директиву 95/46/ЕС в целях, указанных в пункте 1 настоящей статьи. Более того, положения настоящей Директивы предусматривают защиту законных интересов абонентов, являющихся юридическими лицами.

3. Настоящая Директива не должна применяться в отношении видов деятельности, которые выходят за пределы регулирования Договора об учреждении Европейского Сообщества, таких как те, что подпадают под действие разделов V и VI Договора о Европейском Союзе, и в любом случае не должна применяться в отношении видов деятельности, касающихся общественной безопасности и обороны, государственной безопасности (включая экономическое благосостояние государства, когда речь идет о делах государственной безопасности) и в отношении деятельности государства в областях уголовного права.

## Статья 2 Определения\*(10)

Если не предусмотрено иное, определения, содержащиеся в Директиве 95/46/ЕС и в Директиве 2002/21/ЕС Европейского парламента и Совета ЕС от 7 марта 2002 г. об общих рамках регулирования электронных коммуникационных сетей и услуг (Рамочная Директива\*(11)), подлежат применению.

Также подлежат применению следующие определения:

(a) под **"пользователем"** понимается любое физическое лицо, которое потребляет услуги электронной связи общего доступа в личных или деловых целях без обязательной предварительной подписки на предоставление таких услуг;

(b) под **"данными трафика"** понимаются данные, обработанные в целях осуществления передачи сообщения по сети электронной связи или в целях формирования счета за пользование услугами электронной связи;

(c) под **"данными местоположения"** понимаются любые данные, обработанные в сети электронной связи или службой предоставления услуг электронной связи, отражающие географическое местоположение конечной станции пользователя общедоступных услуг;

(d) под **"сообщением"** понимается любая информация, которой обмениваются или которая передается между ограниченным кругом лиц посредством общедоступных услуг электронной связи. В это понятие не включается информация, передаваемая в рамках широкого оповещения общественности по сети электронной связи, за исключением случаев, когда передаваемая информация может иметь отношение к определенному пользователю или абоненту, получающему эту информацию;

(f) **"согласие"** абонента или пользователя соответствует определению согласия в отношении данных в Директиве 95/46/ЕС;

(g) под **"дополнительной услугой"** понимается любая услуга, требующая обработки данных трафика или данных местоположения, являющихся дополнительными к тем данным, которые необходимы для передачи сообщения или формирования счетов за пользование связью;

(h) под **"электронной почтой"** понимается любое текстовое, голосовое, звуковое или графическое сообщение, посланное через общедоступную сеть связи, которое может храниться в сети или на терминальном оборудовании получателя до того момента, как оно будет принято получателем;

(i) под **"повреждением системы безопасности персональных данных"** понимается повреждение безопасности, приводящее к случайному или незаконному уничтожению, потере, изменению, несанкционированному раскрытию или доступу к персональным данным, переданным, сохраненным или обработанным иным образом в связи с предоставлением общедоступных услуг электронной связи в Сообществе.

## Статья 3 Услуги, на которые распространяется настоящая Директива

Настоящая директива должна применяться в отношении обработки персональных данных в связи с предоставлением общедоступных услуг электронной связи в сетях связи коллективного доступа в Сообществе, в том числе в сетях связи коллективного доступа, поддерживающих сбор данных и устройства идентификации.

## Статья 4 Безопасность обработки данных

1. Провайдер общедоступных услуг электронной связи должен предпринять необходимые технические и организационные меры для обеспечения безопасности предоставляемых услуг, при необходимости совместно с провайдером сети связи общего доступа, если это касается вопроса безопасности сети. Принимая во внимание уровень развития

технологий и стоимость их внедрения, данные меры должны гарантировать уровень безопасности, соответствующий имеющимся угрозам.

1а. Не нарушая Директивы 95/46/ЕС, меры, упоминаемые в пункте 1 настоящей статьи, должны по меньшей мере:

- гарантировать, что доступ к персональным данным может быть предоставлен только уполномоченному персоналу в разрешенных законом целях,

- защищать персональные данные, сохраненные или переданные, от случайного или незаконного уничтожения, случайной потери или изменения, несанкционированного или незаконного хранения, обработки, доступа или раскрытия и

- гарантировать введение политики безопасности в отношении обработки персональных данных.

Соответствующие национальные органы власти должны иметь возможность проверить меры, принятые провайдерами общедоступных услуг электронной связи и издать рекомендации о лучших достижениях в отношении уровня безопасности, полученных в результате принятых мер.

2. При наличии определенной угрозы повреждения системы безопасности сети, провайдер общедоступных услуг электронной связи должен информировать абонентов в отношении такой угрозы, а в случаях, когда угроза выходит за пределы средств защиты, доступных провайдеру, - о любых возможных средствах защиты, включая информацию о затратах на их приобретение.

3. В случае повреждения системы безопасности персональных данных провайдер общедоступных услуг электронной связи должен без необоснованного промедления довести до сведения компетентных национальных органов власти о таком повреждении.

При наличии вероятности того, что повреждение системы безопасности персональных данных неблагоприятным образом затронет персональные данные или информацию о частной жизни абонента или индивидуального пользователя, провайдер также должен без необоснованного промедления уведомить абонента или индивидуального пользователя о таком повреждении.

Уведомление абонента или индивидуального пользователя о повреждении безопасности персональных данных не требуется, если провайдер продемонстрировал компетентным органам то, что им были приняты необходимые технологические защитные меры, и то, что эти меры были применены в отношении данных, затронутых в результате повреждения системы безопасности. Такие технологические защитные меры должны представить данные, непонятные любому лицу, не имеющему к ним санкционированного доступа.

Без ущерба действию обязательств провайдера по уведомлению абонентов и заинтересованных индивидов, в случаях, когда провайдер еще не уведомил абонента или индивида о повреждении в системе безопасности персональных данных, компетентные национальные органы власти, оценив вероятные отрицательные последствия этого повреждения, могут потребовать от провайдера осуществить такое уведомление.

Уведомление абонента или индивида должно как минимум описывать характер повреждения системы безопасности персональных данных, содержать указание на контактные пункты, где можно получить дополнительную информацию, и на меры, которые могут быть приняты для того, чтобы смягчить возможные неблагоприятные последствия от повреждения в системе безопасности персональных данных. Уведомление, обращенное к национальным компетентным органам власти, должно, кроме того, описывать последствия повреждения системы безопасности персональных данных, меры, предложенные и принятые провайдером в отношении адресата, само повреждение системы безопасности персональных данных.

4. В связи с любыми техническими мерами, принятыми в соответствии с пунктом 5 настоящей статьи, компетентные национальные органы могут принять руководящие положения, и в случае необходимости издать инструкции, касающиеся обстоятельств, при наступлении которых провайдеры услуг обязаны сделать уведомление о повреждении в системе безопасности персональных данных, формате такого уведомления и способе его осуществления. Указанные органы также должны иметь возможность проверить, выполнили ли провайдеры услуг свои обязательства по осуществлению уведомления в соответствии с настоящим пунктом, и наложить соответствующие штрафные санкции, в случае если провайдеры не поступили должным образом.

Провайдеры услуг должны вести учет повреждений в системе безопасности

персональных данных, включая в список факты, связанные с повреждением, последствия повреждения, и принятые меры по восстановлению. Включенные в список факты должны быть достаточными для того, чтобы дать возможность компетентным национальным органам власти проверить их на соответствие положениям пункта 3 настоящей статьи. Данный список должен включать только информацию, необходимую для этой цели.

5. Для обеспечения последовательности выполнения мер, указанных в пунктах 2, 3 и 4 настоящей статьи, Европейская Комиссия может после консультации с Европейским агентством по сетевой и информационной безопасности (ENISA), Рабочей группой по защите личности в связи с обработкой персональных данных, основанной в соответствии со Статьей 29 Директивы 95/46/ЕС, а также Европейским контролирующим органом по защите данных, принять технические исполнительные меры, касающиеся обстоятельств, формата и процедур, применимых к требованиям по информированию и осуществлению уведомления, упоминаемым в настоящей статье. При принятии таких мер Европейская Комиссия должна привлечь всех имеющих отношение к делу заинтересованных лиц для того, чтобы быть информированными о лучших технических и экономических способах реализации настоящей статьи.

Меры, разработанные для того, чтобы исправить несущественные элементы настоящей Директивы, дополняя ее, должны быть приняты в соответствии с регулятивной процедурой с уточнением, содержащимся в пункте 2 статьи 14(а) настоящей Директивы.

## **Статья 5**

### **Конфиденциальность коммуникаций**

1. Государства-члены ЕС в своем национальном законодательстве должны гарантировать конфиденциальность передаваемых сообщений и относящихся к ним данных трафика посредством сети связи общего пользования и общедоступных услуг электронной связи. В частности, они должны запретить прослушивание, несанкционированное подключение, хранение или другие виды перехвата или слежки за сообщениями и относящимися к ним данными трафика лицам, не являющимся пользователями, без согласия заинтересованных пользователей, кроме случаев получения санкционированного разрешения на осуществление этих действий в соответствии с пунктом 1 статьи 15 настоящей Директивы. Положения настоящего пункта не должны препятствовать техническому хранению, необходимому для передачи сообщения, не нарушая принципа конфиденциальности.

2. Пункт 1 настоящей статьи не должен затрагивать законодательно разрешенную запись сообщений и относящихся к ним данных трафика, когда такая запись производится в ходе законной деловой практики для целей предоставления доказательства совершения коммерческой сделки или осуществления любого другого делового взаимодействия.

3. Государства-члены ЕС должны гарантировать, что хранение информации или получение доступа к информации, уже сохраненной на терминальном оборудовании абонента или пользователя, допускается только при условии, что заинтересованный абонент или пользователь дали свое согласие, будучи обеспеченными точной и полной информацией в соответствии с Директивой 95/46/ЕС, помимо прочего, о целях обработки информации. Данное положение не должно препятствовать любому техническому хранению или доступу к информации с единственной целью осуществления передачи сообщения по сети электронной связи, или в случае наличия необходимости оказания провайдером услуги информационного общества соответствующих услуг по явно выраженному запросу абонента или пользователя.

## **Статья 6**

### **Данные трафика**

1. Данные трафика, касающиеся абонентов и пользователей, обработанные и сохраненные провайдером сети связи общего доступа или провайдером общедоступных услуг электронной связи, должны быть уничтожены или сделаны анонимными, если в них нет дальнейшей необходимости для передачи сообщения, без ущерба действию пунктов 2, 3 и 5 настоящей статьи и пункта 1 статьи 15 настоящей Директивы.

2. Данные трафика, необходимые для формирования счетов абонента за пользование связью и межсоединение, могут быть обработаны. Такая обработка допустима только до

истечения периода времени, в течение которого может быть законодательно оспорен счет за услуги или взыскана плата за межсоединение.

3. В целях продвижения услуг электронных коммуникаций или дополнительных услуг провайдер общедоступных услуг электронной связи может осуществлять обработку данных, упоминаемых в пункте 1 настоящей статьи. Данная обработка допускается до той степени и на протяжении такого периода времени, какие необходимы для подобных услуг или маркетинга, при условии, что абонент или пользователь, к которым относятся эти данные, дал свое предварительное согласие на их обработку. Абонентам или пользователям должна быть предоставлена возможность отозвать свое согласие на обработку данных трафика в любое время.

4. Провайдер услуг должен информировать абонента или пользователя о видах данных трафика, находящихся в обработке, и о длительности такой обработки для целей, упоминаемых в пункте 2 настоящей статьи, и до получения согласия, в целях, упоминаемых в пункте 3 настоящей статьи.

5. Обработка данных трафика в соответствии с пунктами 1, 2, 3 и 4 настоящей статьи должна быть ограничена для лиц, действующих под руководством провайдеров сетей связи общего доступа, провайдеров общедоступных услуг электронной связи, в пределах, необходимых для осуществления данными лицами следующих видов деятельности: управления трафиком или биллингом, рассмотрения требований клиентов, обнаружения мошенничества, продвижения услуг электронной связи или предоставления дополнительных услуг.

6. Пункты 1, 2, 3 и 5 настоящей статьи подлежат применению без ущерба действию возможности компетентных органов быть информированными о данных трафика в соответствии с применимым законодательством в целях урегулирования споров, в частности, споров по вопросам межсоединения и биллинга.

## **Статья 7** **Детализирование счетов**

1. Абоненты должны иметь право получать не детализированные счета.

2. Государства-члены ЕС должны применять национальные положения для того, чтобы согласовать права абонентов, получающих детализированные счета, с правом вызывающих пользователей и вызываемых абонентов на неприкосновенность частной жизни, например, путем гарантирования доступности для указанных пользователей или абонентов таких приемлемых альтернативных способов коммуникаций или осуществления платежей, которые повышают безопасность их частной жизни.

## **Статья 8** **Показ и блокирование определения вызывающего и соединенного номеров**

1. В случае, когда предлагается показ определения вызывающего номера, провайдер услуг должен предоставить вызывающему пользователю возможность простыми способами и бесплатно отменить показ определения вызывающего номера в отношении каждого вызова. Вызывающий абонент должен иметь такую возможность в отношении каждого телефонного номера.

2. В случае, когда предлагается показ определения вызывающего номера, провайдер услуг должен предложить вызывающему абоненту возможность обоснованно, бесплатно и простым способом использовать функцию по отмене показа определения вызывающего номера для входящих вызовов.

3. В случае, когда предлагается показ определения вызывающего номера и когда такой показ осуществляется перед тем, как будет установлен вызов, провайдер услуг должен предоставить вызываемому абоненту возможность с использованием простых средств отклонять входящие вызовы, по которым вызывающим абонентом или пользователем был заранее отменен показ определения вызывающего номера.

4. В случае, когда предлагается показ соединенного номера, провайдер услуг должен предоставить вызываемому абоненту бесплатную возможность с использованием простых средств отменять показ соединенного номера для вызывающего пользователя.

5. Пункт 1 настоящей статьи должен также применяться в отношении вызовов, адресованных в третьи страны, появляющиеся в Сообществе. Пункты 2, 3 и 4 настоящей статьи также должны применяться в отношении входящих вызовов в третьих странах.

6. Государства-члены ЕС должны гарантировать, что в случаях, когда предлагается показ вызывающего и/или соединенного номера, провайдер общедоступных услуг электронной связи информирует об этом общественность, а также он информирует о возможностях, установленных в пунктах 2, 3 и 4 настоящей статьи.

## **Статья 9**

### **Данные местоположения, отличные от данных трафика**

1. В случаях, когда допускается возможность обработки данных местоположения, отличных от данных трафика и имеющих отношение к абонентам или пользователям общедоступных услуг электронной связи, такие данные могут быть обработаны только после того, как они будут сделаны анонимными, или с согласия пользователей или абонентов. При этом такая обработка допускается до той степени и в течение такого периода времени, какие необходимы для оказания дополнительных услуг. Провайдер услуг должен информировать пользователей или абонентов перед получением их согласия о типе данных местоположения, отличных от данных трафика, которые будут обрабатываться, о длительности и целях обработки, а также о том, будут ли передаваться данные третьей стороне в целях оказания дополнительных услуг. Пользователям или абонентам должна быть предоставлена возможность в любое время отозвать свое согласие на обработку данных местоположения, отличных от данных трафика.

2. В случае, когда согласие пользователя или абонента на обработку данных местоположения, отличных от данных трафика, уже получено, у пользователя или абонента должна сохраняться возможность простым способом и бесплатно временно отказаться от обработки таких данных применительно к каждому соединению с сетью или каждой передаче сообщения.

3. Обработка данных местоположения, отличных от данных трафика в соответствии с пунктами 1 и 2 настоящей статьи, должна быть ограничена для лиц, действующих под руководством провайдера сети связи общего доступа или провайдера общедоступных услуг электронной связи или третьей стороны, предоставляющей дополнительные услуги. Данное ограничение должно осуществляться до пределов, необходимых для предоставления дополнительных услуг.

## **Статья 10**

### **Исключения**

Государства-члены ЕС должны гарантировать, что существуют прозрачные процедуры, регулирующие способ, которым провайдер сети связи общего пользования и/или общедоступных услуг электронной связи может устранить:

(a) временную отмену показа определения вызывающего номера по заявлению абонента, требующего отслеживания злонамеренных вызовов или вызовов, создающих помехи. В этом случае в соответствии с национальным законодательством данные номера вызывающего абонента, будут сохраняться и будут сделаны доступными провайдером сети связи общего пользования и/или общедоступных услуг электронной связи;

(b) отмену показа определения номера вызывающего абонента и временный отказ или отсутствие согласия абонента или пользователя на обработку данных местоположения в отношении каждого телефонного номера для организаций, имеющих дело с экстренными вызовами и признаваемыми таковыми государством-членом ЕС, в том числе для правоохранительных органов, служб скорой медицинской помощи, пожарных команд в целях реагирования на такие вызовы.

## **Статья 11**

### **Автоматический повтор вызова**

Государства-члены ЕС должны гарантировать, что любой абонент имеет возможность простым способом и бесплатно остановить автоматический повтор вызова, посылаемого на терминальное оборудование абонента третьей стороной.

## **Статья 12**

### **Справочники абонентов**

1. Государства-члены ЕС должны гарантировать, что абоненты перед включением их в справочник бесплатно проинформированы о цели (целях) печатного или электронного справочника абонентов, находящегося в свободном доступе или запрашиваемого через справочные службы, в которые могут быть включены их персональные данные, и о любых дальнейших возможностях использования данных, основанных на функциях поиска, встроенных в электронные версии справочника.

2. Государства-члены ЕС должны гарантировать, что абонентам предоставлена возможность определять, включены ли их персональные данные в общедоступный справочник. Если персональные данные абонентов включены в общедоступный справочник, то абонентам должна быть предоставлена возможность определять, до какой степени эти данные имеют отношение к целям справочника, определенным поставщиком справочника, а также возможность проверять, вносить исправления в данные или отзываться такие данные. Отказ абонентов от включения их данных в общедоступный справочник абонентов, проверка персональных данных, внесение в них исправлений или отзыв персональных данных из справочника абонентов должны осуществляться бесплатно.

3. Государства-члены ЕС могут потребовать, чтобы для любых целей общедоступного справочника, иных, чем поиск деталей контакта людей на базе их имени и необходимого минимального количества других идентификационных признаков, было запрошено дополнительное согласие абонентов.

4. Пункты 1 и 2 настоящей статьи должны применяться в отношении абонентов, являющихся физическими лицами. Государства-члены ЕС также должны гарантировать в рамках законодательства Сообщества и применимого национального законодательства, что законные интересы абонентов, не являющихся физическими лицами, в связи с внесением их в общедоступные справочники достаточно защищены.

## **Статья 13**

### **Незапрашиваемые сообщения**

1. Использование систем связи автоматического повтора вызова без человеческого вмешательства (устройства автоматического дозвона), факсимильных аппаратов (факсов) или электронной почты в целях прямого маркетинга допускается только в отношении абонентов или пользователей, давших свое предварительное согласие.

2. Несмотря на положения пункта 1 настоящей статьи, в случаях когда физическое или юридическое лицо получает от своих клиентов адрес электронной почты в связи с продажей товара или оказанием услуги, в соответствии с Директивой 95/46/ЕС то же самое физическое или юридическое лицо может использовать эти адреса в целях прямого маркетинга своих собственных аналогичных товаров и услуг при условии, что клиентам ясно и отчетливо предоставляется возможность возражать бесплатно и простым способом против такого использования их электронных адресов во время предоставления ими своих адресов и при получении ими каждого сообщения в том случае, если клиент первоначально не отказался от использования своего электронного адреса.

3. Государства-члены ЕС должны принять соответствующие меры для гарантии недопущения отправки незапрашиваемых сообщений в целях прямого маркетинга, в случаях иных, чем те, что упоминаются в пунктах 1 и 2 настоящей статьи, как без согласия заинтересованных абонентов и пользователей, так и в отношении абонентов или пользователей,

не желающих получать такие сообщения.

Государства-члены ЕС также должны принять меры для определения разницы в национальном законодательстве между этими двумя возможностями неполучения абонентами незапрашиваемых сообщений, принимая в расчет, что обе эти возможности должны быть бесплатными для абонента или пользователя.

4. В любом случае должна быть запрещена практика отправки в целях прямого маркетинга электронной почты, маскирующей или скрывающей идентификацию отправителя в нарушение Статьи 6 Директивы 2000/31/ЕС, отправка сообщений с недействительного адреса, на который получатель не может отправить запрос о прекращении отправки таких сообщений, либо отправка в нарушение указанной статьи почты, побуждающей получателей посещать вэб-сайты.

5. Пункты 1 и 3 настоящей статьи должны применяться в отношении абонентов, являющихся физическими лицами. Государства-члены ЕС должны также гарантировать, в рамках законодательства Сообщества и применимого национального законодательства, что законные интересы абонентов, не являющихся физическими лицами, в отношении незапрашиваемых сообщений достаточно защищены.

6. Без предубеждения к любому административному средству защиты права, которое может быть создано, *inter alia*, в соответствии с пунктом 2 Статьи 15а настоящей Директивы, государства-члены ЕС должны гарантировать, что любое физическое или юридическое лицо, ощутившее на себе неблагоприятные последствия нарушений национальных положений, принятых согласно настоящей статье и в связи с этим имеющих законный интерес в прекращении или запрещении подобных нарушений, включая провайдера услуг электронной связи, защищающего свои законные деловые интересы, может начать судебное разбирательство в отношении таких нарушений. Государства-члены ЕС могут также установить особые правила о штрафах, применимых к провайдерам услуг электронной связи, которые в результате своей небрежности способствуют нарушению национальных положений, принятых в соответствии с настоящей статьей.

## **Статья 14**

### **Технические характеристики и стандартизация**

1. При реализации положений настоящей Директивы государства-члены ЕС должны гарантировать применительно к пунктам 2 и 3 настоящей статьи, что на терминальное или иное оборудование для электронной связи не налагаются обязательные требования к особым техническим характеристикам, которые могут препятствовать размещению оборудования на рынке и свободному обращению такого оборудования как в отдельном государстве-члене ЕС, так и между государствами-членами ЕС.

2. В случаях, когда условия настоящей Директивы могут быть реализованы только при предъявлении особых требований к техническим характеристикам в сетях электронной связи, государства-члены ЕС должны информировать об этом Европейскую Комиссию в соответствии Директивой 98/34/ЕС Европейского парламента и Совета ЕС от 22 июня 1998 г. о процедуре предоставления информации в области технических стандартов и регламентов, а также правилах оказания услуг в информационном обществе\*(12).

3. В случае необходимости могут быть приняты меры для гарантии того, что терминальное оборудование сконструировано таким образом, чтобы обеспечивать право пользователей на защиту и осуществление контроля использования их персональных данных в соответствии с Директивой 1999/5/ЕС и Решением 87/95/ЕЭС Совета ЕС от 22 декабря 1986 г. о стандартизации в сфере информационных технологий и коммуникаций\*(13).

## **Статья 14а**

### **Порядок взаимодействия с Комитетом по связи**

1. Европейской Комиссии должна быть оказана помощь Комитетом по связи, образованным в соответствии со Статьей 22 Директивы 2002/21/ЕС (Рамочная Директива).

2. При ссылке на настоящий пункт, подлежат применению пункты 1 - 4 Статьи 5а и Статья 7 Решения 1999/468/ЕС, имеющие отношение к положениям Статьи 8 данного

документа.

3. При ссылке на настоящий пункт, подлежат применению пункты 1, 2, 4 и 6 Статьи 5а и Статья 7 Решения 1999/468/ЕС, имеющие отношение к положениям Статьи 8 данного документа.

## **Статья 15**

### **Применение отдельных положений Директивы 95/46/ЕС**

1. Государства-члены ЕС могут принять законодательные меры для ограничения области прав и обязанностей, предусмотренных Статьями 5, 6, пунктами 1, 2, 3 и 4 Статьи 8 и Статьи 9 настоящей Директивы, если такое ограничение представляет собой необходимую, соответствующую и пропорциональную меру в рамках демократического общества для осуществления защиты национальной (государственной) безопасности, обороны и общественной безопасности, предотвращения, расследования, обнаружения и судебного преследования преступных действий или несанкционированного использования системы электронной связи, как об этом говорится в пункте 1 статьи 13 Директивы 95/46/ЕС. В связи с этим государства-члены ЕС могут, помимо прочего, принять законодательные меры, предусматривающие сохранение данных на определенный период по основаниям, предусмотренным в настоящем пункте. Все меры, упоминаемые в настоящем пункте, должны находиться в соответствии с общими принципами законодательства Сообщества, включая те, что содержатся в пунктах 1 и 2 Статьи 6 Договора о Европейском Союзе.

1а. Пункт 1 настоящей статьи не должен применяться к данным, в отношении которых Директивой 2006/24/ЕС Европейского парламента и Совета ЕС от 15 марта 2006 г. об удержании данных, генерированных или обработанных в связи с оказанием общедоступных услуг электронной связи или сетей связи общего доступа\*(14), предъявляются требования по их удержанию в целях, указанных в пункте 1 Статьи 1 названной Директивы.

1b. Провайдеры услуг должны установить внутренние процедуры для ответа на запросы о предоставлении доступа к персональным данным пользователя, основанные на национальных положениях, принятых в соответствии с пунктом 1 настоящей статьи. Они должны обеспечить компетентные национальные органы власти по их требованию информацией об этих процедурах, количестве полученных запросов, примененных правовых обоснованиях и информацией о своих ответных действиях.

2. Положения Раздела III о судебных средствах защиты, ответственности и санкциях, предусмотренных Директивой 95/46/ЕС, должны применяться в связи с учетом национальных положений, принятых в соответствии с настоящей Директивой и с учетом прав индивидов, проистекающих из настоящей Директивы.

3. Рабочая группа по защите личности в связи с обработкой персональных данных, созданная на основании Статьи 29 Директивы 95/46/ЕС, также должна решать задачи, поставленные в Статье 30 указанной Директивы, связанные с вопросами, входящими в сферу регулирования настоящей Директивы, а именно защиты основных прав, свобод и законных интересов в сфере электронных коммуникаций.

## **Статья 15а**

### **Применение и вступление в силу**

1. Государства-члены ЕС должны установить нормы о штрафах, включая при необходимости санкции за совершение преступлений, применяемые за нарушения национальных положений, принятых в соответствии с настоящей Директивой, а также принять все меры, необходимые для реализации указанных санкций. Предусмотренные штрафы должны быть эффективными, пропорциональными и сдерживающими и могут быть применены в период совершения любого нарушения, даже в случаях когда последствия нарушения были впоследствии устранены. Государства-члены ЕС должны уведомить об этих положениях Европейскую Комиссию в срок до 25 мая 2011 г. без задержек, которые могут возникнуть в связи с принятием впоследствии любых касающихся их поправок.

2. Без ущерба действию любого доступного средства судебной защиты, государства-члены ЕС должны гарантировать, что компетентные национальные органы власти

и другие имеющие отношение к делу национальные органы имеют полномочия давать указания о прекращении нарушений, упоминаемых в пункте 1 настоящей статьи.

3. Государства-члены ЕС должны гарантировать, что компетентные национальные органы власти и другие соответствующие национальные органы имеют необходимые следственные полномочия и ресурсы, включая полномочие на получение любой имеющей отношение к делу информации, которая может им понадобиться для отслеживания и реализации национальных положений, принятых в соответствии с настоящей Директивой.

4. Соответствующие национальные регулирующие органы могут принять меры для обеспечения эффективной трансграничной кооперации по реализации национальных законодательных актов, принятых в соответствии с настоящей Директивой, и создать согласованные условия для оказания услуг, включающих трансграничный обмен потоками данных.

Национальные регулирующие органы должны обеспечить Европейскую Комиссию заблаговременно перед принятием любой из этих мер кратким отчетом, содержащим перечень оснований для осуществления действий, предусмотренные меры и предложенный способ действия. Европейская Комиссия, изучив данную информацию и получив консультацию Европейского агентства по сетевой и информационной безопасности (ENISA) и Рабочей группы по защите личности в связи с обработкой персональных данных, созданной на основании Статьи 29 Директивы 95/46/ЕС, может вслед за этим дать свои комментарии или рекомендации, в частности, для обеспечения гарантий того, что предусмотренные меры не скажутся неблагоприятным образом на функционировании международного рынка. Национальные регулирующие органы при выборе мер должны предельным образом учитывать рекомендации и комментарии Европейской Комиссии.

## **Статья 16**

### **Переходные меры**

1. Статья 12 настоящей Директивы не должна применяться в отношении выпусков справочников, уже изготовленных или размещенных на рынке в печатной или электронной форме прежде, чем национальные положения, принятые в соответствии с настоящей Директивой, вступят в силу.

2. В случаях, когда персональные данные абонентов услуг стационарной или мобильной общедоступной голосовой телефонии были включены в общедоступный справочник абонентов в соответствии с положениями Директивы 95/46/ЕС и Статьей 11 Директивы 97/66/ЕС перед тем, как национальные положения, принятые согласно настоящей Директиве, вступили в силу, персональные данные таких абонентов могут оставаться включенными в этот справочник в его печатной или электронной версиях, включая версии с функциями поиска, до тех пор пока абоненты не изъявят об их исключении из справочников, получив информацию о целях и возможностях в соответствии со Статьей 12 настоящей Директивы.

## **Статья 17**

### **Преобразование в национальное право**

1. До 31 октября 2003 г. государства-члены ЕС должны ввести в действие положения, необходимые для исполнения настоящей Директивы, и немедленно сообщить об этом Европейской Комиссии.

Указанные положения, принятые государствами-членами ЕС, должны содержать ссылку на настоящую Директиву или сопровождаться такой ссылкой в случае их официального опубликования. Способы, которыми может быть сделана данная ссылка, должны устанавливаться государствами-членами ЕС.

2. Государства-члены ЕС должны довести до сведения Европейской Комиссии текст положений национального законодательства, принимаемого ими в сфере регулирования настоящей Директивы и любых последующих изменений этих положений.

## **Статья 18**

### **Пересмотр**

Европейская Комиссия должна представить Европейскому парламенту и Совету ЕС не позднее трех лет по истечении даты, упоминаемой в пункте 1 Статьи 17 настоящей Директивы отчет о применении Директивы и ее влиянии на экономических агентов и потребителей, в особенности положений, касающихся незапрашиваемых сообщений, принимая во внимание международную среду. Для этой цели Европейская Комиссия может затребовать от государств-членов ЕС информацию, которая должна быть предоставлена без неоправданной задержки. При необходимости Европейская Комиссия должна представить предложения о внесении изменений в настоящую Директиву, учитывая результаты данного отчета, любые изменения в сфере электронных коммуникаций и любое иное предложение, которое она сочтет необходимым для повышения эффективности настоящей Директивы.

## **Статья 19**

### **Отмена**

Директива 97/66/ЕС тем самым утрачивает силу с даты, указанной в пункте 1 Статьи 17 настоящей Директивы.

Ссылки, сделанные на утратившую силу Директиву, должны рассматриваться как ссылки, сделанные на настоящую Директиву.

## **Статья 20**

### **Вступление в силу**

Настоящая Директива вступает в силу в день ее опубликования в Официальном Журнале Европейского Сообщества.

## **Статья 21**

### **Адресаты**

Настоящая Директива адресована государствам-членам ЕС.

Совершено в Брюсселе, 12 июля 2002 г.

За Европейский Парламент  
Президент  
P. Cox

За Совет ЕС  
Президент  
T. Pedersen

---

\*(1) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Опубликовано в Официальном журнале (далее - ОЖ) N L 201, 31.7.2002, стр. 37.

\*(2) ОЖ N C 365 E, 19.12.2000, стр. 223.

\*(3) ОЖ N C 123, 25.04.2001, стр. 53.

\*(4) Заключение Европейского парламента от 13 ноября 2001 г. (еще не опубликованное в Официальном журнале), Общая позиция Совета ЕС от 28 января 2002 г. (ОЖ N C 113 E, 14.05.2002, стр. 39) и Решение Европейского парламента от 30 мая 2002 г. (еще не опубликованное в Официальном журнале). Решение Совета ЕС от 25 июня 2002 г.

\*(5) ОЖ N L 281, 23.11.1995, стр. 31.

\*(6) ОЖ N L 24, 30.1.1998, стр. 1.

\*(7) Cookies - идентификационные файлы Интернет, сохраняемые на терминальном оборудовании пользователя, позволяющие сохранять индивидуальную информацию о пользователе сети - прим. перев.

\*(8) ОЖ N L 178, 17.07.2000, стр. 1.

\*(9) ОЖ N L 91, 07.04.1999, стр. 10.

\*(10) Часть пунктов статьи удалена актами, вносящими изменения - прим. перев.

\*(11) ОЖ N L 108, 24.04.2002, стр. 33.

\*(12) ОЖ N L 204, 21.07.1998, стр. 37. Текст в редакции Директивы 98/48/ЕС (ОЖ N L 217, 05.08.1998, стр. 18).

\*(13) ОЖ N L 36, 07.02.1987, стр. 31. Текст в редакции Акта о присоединении 1994 г.

\*(14) ОЖ N L 105, 13.04.2006, стр. 54.