

УДК 006.033:004.056.5

Фаль А.М.

ДИНАМИКА ТРЕБОВАНИЙ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ЗАКОНОДАТЕЛЬСТВЕ ЕВРОПЕЙСКОГО СОЮЗА

Анотація:

У повідомленні розглянуто процес змін у законодавстві Європейського Союзу стосовно захисту персональних даних. Директива 95/46/ЕС започаткувала формулювання вимог щодо захисту персональних даних. Цьогорічний документ стосується вимог щодо сповіщення зацікавлених сторін про порушення у сфері захисту персональних даних.

Аннотация:

В сообщении рассмотрен процесс изменений в законодательстве Европейского Союза по защите персональных данных. Директива 95/46/ЕС впервые сформулировала требования по защите персональных данных. Документ этого года касается требований к уведомлению заинтересованных сторон о нарушениях в сфере защиты персональных данных.

Abstract:

The report describes the process of the changes in legislation of the European Union concerning the protection of personal data. Directive 95/46/EC started formulate requirements for the protection of personal data. This year's document relates to the requirements for notification of interested parties on the breach of the protection of personal data.

Основополагающим документом в сфере защиты персональных данных является Директива 95/46/ЕС [1]. Ее положения были конкретизированы в Директиве 97/66/ЕС [2] применительно к сектору телекоммуникаций. Бурное развитие цифровых технологий заставило принять новую Директиву 2002/58/ЕС [3] взамен предыдущей. Сфера ее применения охватывает предоставление услуг электронных коммуникаций в различных средах, включая Интернет, мобильную связь и т.п.

Статья 4 этой директивы касается вопросов обеспечения безопасности (security). В ней утверждается, что поставщик услуг электронных коммуникаций должен предпринять технические и организационные меры по обеспечению безопасности, уровень которой соответствует существующему риску. Поставщик услуг, который не в состоянии устранить конкретный риск нарушения безопасности в случае его наличия, должен известить об этом потребителей услуг.

В 2009 году была принята Директива 2009/136/ЕС [4], в которой сформулированы изменения, касающиеся трех директив. Рассмотрим интересующие нас изменения, внесенные в Директиву 2002/58/ЕС. В статье 2, касающейся определений, введено новое понятие «нарушение персональных данных», обозначающее нарушение безопасности, ведущее к случайным или незаконным разрушениям, потерям, изменениям, неуполномоченному раскрытию или доступу к персональным данным, которые передаются, хранятся или обрабатываются в связи с предоставлением услуги электронных сообщений.

Положения статьи 4, касающейся обеспечения безопасности, уточнены и расширены. В частности, утверждается, что предпринимаемые меры по обеспечению безопасности должны:

- обеспечивать то, что персональные данные должны быть доступны лишь для уполномоченных лиц и для разрешенных целей;
- защищать хранимые или обрабатываемые персональные данные от случайных или незаконных разрушений, потерь, изменений, неуполномоченного раскрытия или доступа к ним;
- обеспечивать выполнение политики безопасности, касающейся обработки персональных данных.

В случае нарушения персональных данных поставщик услуг обязан без проволочки извещать об этом национальный компетентный орган. Если нарушение персональных данных может нанести вред потребителю услуг или субъекту персональных данных, поставщик услуг обязан также извещать их о нарушении.

Для обеспечения согласованности в реализации изложенных выше мер Комиссия ЕС может принять технические способы реализации мер, касающиеся обстоятельств, форматов, процедур, применимых к изложенным выше требованиям по извещению о нарушениях.

В развитие этого в стадии утверждения находится проект документа [5] прямого действия. Статья 2 этого документа утверждает, что поставщик услуг должен известить о нарушении персональных данных национальный компетентный орган не позже, чем через 24 часа после обнаружения нарушения персональных данных, если это выполнимо. Формат извещения приведен в Дополнении 1.

Если не доступна полная информация Дополнения 1 и требуется дополнительное расследование нарушения персональных данных, поставщику должно быть разрешено сделать начальное извещение обнаружения нарушения персональных данных. Это начальное извещение национального компетентного органа должно содержать информацию раздела 1 Дополнения 1. Поставщик должен сделать второе извещение как можно скорее и не позже трех дней после начального извещения. Это второе извещение должно содержать информацию раздела 2 Дополнения 1. Если поставщик, несмотря на проведенное расследование, не в состоянии предоставить полную информацию в трехдневный срок по-

сле начального извещения, поставщик должен представить в этот срок максимальное количество имеющейся у него информации.

Национальный компетентный орган должен обеспечить поставщика услуг надежными электронными средствами для извещения о нарушении персональных данных и информацией о процедурах, доступе к ним и об их использовании.

Если нарушение персональных данных может нанести вред потребителю или субъекту персональных данных, поставщик услуг должен также известить потребителя или субъекта персональных данных. Формат извещения потребителя о нарушении персональных данных приведен в Дополнении 2.

В исключительных обстоятельствах, когда извещение потребителя о нарушении персональных данных может создать риск должному расследованию нарушения персональных данных, поставщику может быть разрешено после согласования с национальным компетентным органом отложить извещение о нарушении персональных данных на время, которое национальный компетентный орган считает возможным для задержки извещения.

В настоящее время в сообществе Европейского Союза обсуждается вопрос замены Директивы 95/46/ЕС новым документом (Regulation), имеющим прямое действие.

Литература:

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [Electronic Resource] // Official Journal. – 1995. – L 281, 23.11.1995. – P. 31–50. – Mode of access:

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>.

2. Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector [Electronic Resource] // Official Journal. – 1998. – L 24, 30.1.1998. – P. 1–8. – Mode of access: http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31997L0066&model=guichett.

3. 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) [Electronic Resource] // Official Journal. – 2002. – L 201, 31.07.2002. – P. 37–47. – Mode of access: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0037:EN:PDF>.

4. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [Electronic Resource] // Official Journal. – 2009. – L 337, 18.12.2009. – P. 11–36. – Mode of access: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF>.

5. Commission regulation (EU) N / of XXX on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC on privacy and electronic communications. Telecom 44. Dataprotect 31. [Electronic Resource]. – Mode of access: http://www.parlament.gv.at/PAKT/EU/XXIV/EU/10/85/EU_108581/imfname_10395930.pdf.