ДОПОЛНЕНИЕ
к информации JDC относительно персональных данных подопечных Хэсэдов.

1. Основные обязанности Хэсэда, как организации обрабатывающей персональные данные (обязанности оператора ПД).

Помимо изложенного в информационном сообщении JDC относительно возможности обработки ПД только с согласия подопечных и необходимости защиты этих данных в соответствии с рекомендациями JDC, в обязанности оператора ПД входит:

- обеспечение защиты обрабатываемых персональных данных в соответствии с требованиями, установленными соответствующими нормативными актами.

Требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (т.е. программная защита информационных баз данных), требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных, определяется Правительством РФ. При этом, Постановлением Правительства РФ от 17.11.2007 г. №781 *(см.ссылку ниже)* обязанность классификации используемых информационных систем персональных данных и обеспечение их защиты в зависимости от категории персональных данных, возложена соответственно на лицо, обрабатывающее персональные данные - на Хэсэды. Классификация информационных систем персональных данных по степени защиты персональных данных должны осуществляться в соответствии с Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» *(см.ссылку ниже)* в зависимости от категории обрабатываемых данных и их количества.

Категории персональных данных установлены в частности п.6 «Порядка проведения классификации информационных систем персональных данных», утв. Приказом Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13.02.2008 г. №55/86/20.

Особенности обеспечения мер безопасности при обработке персональных данных подопечных без использования средств автоматизации (в т.ч. на бумажных носителях, бланках, формах), а так же извлеченных из автоматизированных средств обработки данных (распечатанных из баз данных) и в дальнейшем обрабатываемые при непосредственном участии человека, регламентируются Постановлением Правительства РФ от 15.09.2008 г. №687 *(см.ссылку ниже),* утвердившим соответствующее Положение. При этом, использование и хранение биометрических персональных данных вне информационных систем персональных данных (вне информационной компьютерной базы данных) могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения (ч.4 ст.19 ФЗ «О персональных данных»).

Особого внимания заслуживают Письма Федерального агентства по образованию от 29.07.2009 г. №17-110 и от 22.10.2009 г. №17-187 «Об обеспечении защиты персональных данных», содержащие конкретную информацию об основных нормативно-методических документах и требованиях по организации защиты персональных данных.

Согласно этим письмам, в настоящее время законодательно-нормативная база по персональным данным в том числе (сделана выборка наиболее принципиальных и важных нормативных актов и ссылок) включает:

- Федеральный закон Российской Федерации от 27.07.2006 г. N 152-ФЗ "О персональных данных".

http://www.rsoc.ru/main/directions/874/916.shtml
http://www.fstec.ru/_razd/_ispo.htm

- Трудовой кодекс Российской Федерации от 30.12.2001 г. N 197-ФЗ (14 глава, с изменениями и дополнениями)
http://www.rsoc.ru/main/directions/874/916.shtml
http://www. consultant.ru/popular/tkrf/

- Постановление Правительства Российской Федерации от 17.11.2007 г. N 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных"
http://www.rg.ru/2007/11/21/personalnye-dannye-dok.html
http://www.garant.ru/hotlaw/doc/106330.htm

- Постановление Правительства Российской Федерации от 15.09.2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"
http://www.rg.ru/2008/09/24/dannye-obrabotka-dok.html
http://www.garant.ru/hotlaw/doc/122316.htm

- Постановление Правительства Российской Федерации от 6.07.2008 г. N 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных"
http://www.rg.ru/2008/07/11/trebovaniya-dok.html
http://www.garant.ru/hotlaw/doc/117878.htm

- Постановление Правительства Российской Федерации от 15.08.2006 г. N 504 «О лицензировании деятельности по технической защите конфиденциальной информации»
http://www.fstec.ru/_razd/_ispo.htm
http://infopravo.by.ru/fed2005/ch01/akt11179.shtm

- Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 г. N 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных"
http://www.fstec.ru/_docs/_perech2.htm
http://www.rg.ru/2008/04/12/informaciya-doc.html

- Приказ Россвязькомнадзора от 17.07.2008 г. N 08 "Об утверждении образца формы уведомления об обработке персональных данных" и от 18.02.2009 N 42 "О внесении изменений в приказ Россвязькомнадзора от 17 июля 2008 г. N 8 "Об утверждении образца формы уведомления об обработке персональных данных"
http://www.rsoc.ru/main/directions/874/916.shtml
http://www.rsoc.ru/main/directions/874/916.shtml

- уведомление уполномоченного федерального органа о деятельности, связанной с обработкой персональных данных для включения оператора ПД в гос. реестр.

Согласно ст.22 ФЗ «О персональных данных». Хэсэды, до начала обработки персональных данных подопечных (т.е. до начала сбора данных в т.ч.) обязаны уведомить уполномоченный орган по защите прав субъектов персональных данных (территориальный орган Федеральной службы по надзору в сфере связи) о своем намерении осуществлять обработку персональных данных.

Понятно, что Хэсэды осуществлявшие обработку ПД до вступления в силу ФЗ «О персональных данных» не освобождаются от обязанности произвести такое уведомление.

Анализ характера и содержания обрабатываемых Хэсэдами персональных данных, исключающих общедоступный характер этой информации, позволяет отнести их к специальной категории информации, требующей предварительного письменного согласия субъекта персональных данных (подопечного) и повышенных мер защиты информационных систем, содержащих базу персональных данных подопечных. Данное обстоятельство обуславливает обязательный характер уведомления уполномоченного органа о намерении осуществлять обработку (или об осуществлении обработки) персональных данных такой категории.

Необходимо отметить, что согласно ч.2 ст.22 ФЗ «О персональных данных», применительно к Хэсэдам, можно рассматривать случаи обработки персональных данных, **не требующие уведомления**, а именно случаи обработки данных:

- относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения (штатные работники Хэсэда). Представляется, что волонтеры к данной категории субъектов персональных данных не относятся;
- относящихся к членам (участникам) Хэсэда, общественного объединения и обрабатываемых самим Хэсэдом в соответствии с целями создания, согласно учредительным документам и действующему законодательству РФ, при условии, что такие персональные данные не будут распространяться (делаться общедоступными на сайте Хэсэда, передаваться третьим лицам (донорам, благотворителям), публикуются в СМИ) без согласия в письменной форме указанных субъектов персональных данных;
- полученных Хэсэдом в связи с заключением разового договора, стороной которого является подопечный, как субъект персональных данных, если его персональные данные не распространяются (не передаются донорам, не публикуются в СМИ и Интернете), а также не предоставляются третьим лицам без отдельного письменного согласия субъекта персональных данных и используются Хэсэдом исключительно для исполнения данного договора;

Цель указанного Уведомления – включение Хэсэда (в 30-ти дневный срок с даты уведомления) в государственный реестр операторов персональных данных для последующего контроля за соблюдением Хэсэдом требований действующего законодательства (ч.4 ст.22 ФЗ «О персональных данных»). Положение «О ведении реестра операторов, осуществляющих обработку персональных данных» утверждено Приказом Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия от 28.03.2008 г. №154.

Указанное Уведомление должно быть направлено в письменной форме и подписано уполномоченным лицом (директором Хэсэда) или направлено в электронной форме и подписано электронной цифровой подписью в соответствии с законодательством РФ. Уведомление должно содержать следующие сведения:

- наименование и адрес места нахождения Хэсэда, как оператора персональных данных;
- цель обработки персональных данных *(напр.: установление нуждаемости подопечных в получении того или иного вида помощи от Хэсэда в целях оказания медико-социальных услуг)*;
- категории персональных данных *(см. п.6 «Порядка проведения классификации информационных систем персональных данных», утв.Приказом Федеральной службы по техническому и экспортному контролю, ФСБ РФ и Министерства информационных технологий и связи РФ от 13.02.2008 г. №55/86/20.)*;
- категории субъектов, персональные данные которых обрабатываются *(описание социальной группы подопечных: малоимущие, одинокие, нуждающиеся в оказании материальной и иной поддержке, проживающие на территории места нахождения Хэсэда и т.д.)*;
- правовое основание обработки персональных данных (*к уведомлению прилагаются копии правоустанавливающих документов Хэсэда: Устав, Свидетельство о государственной регистрации (присвоение ОГРН), Свидетельство о постановке на налоговый учет (присвоение ИНН) и локальный нормативный акт Хэсэда, из категории документов внутреннего распорядка деятельности организации, регламентирующий порядок и условия работы с персональными данными штатных сотрудников Хэсэда, персональными данными участников Хэсэда, как общественной организации и персональными данными подопечных. Видимо это должно быть соответствующее Положение «О работе с персональными данными»*);
- перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных *(напр.: формирование информационной базы персональных данных подопечных Хэсэда с использованием программных средств, с последующим возможным распространением путем передачи персональных данных подопечных полностью или в части донорам и благотворителям в составе отчетов о выполнении благотворительных программ, с возможной трансграничной передачей персональных данных зарубежным донорам (Джойнт), с возможной публикацией персональных данных подопечных полностью или в части в СМИ (печатных изданиях и на общедоступном сайте Хэсэда)*;
- описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению защищенности персональных данных при их обработке (*в зависимости от категории персональных данных и ориентировочного количества подопечных, чьи данные будут обрабатываться; см. Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»*);
- дата начала обработки персональных данных (*дата начала сбора персональных данных*);

- срок или условие прекращения обработки персональных данных (*напр.: по завершению исполнения конкретной благотворительной программы; вар.: в течение всего периода деятельности Хэсэда по осуществлению уставной деятельности в соответствии с действующим законодательством*).

Форма вышеуказанного уведомления рекомендована Приказами Россвязькомнадзора от 17.07.2008 г. №08 «Об утверждении образца формы уведомления об обработке персональных данных» с изменениями, внесенными Приказом от 18.02.2009 №42 (ссылки см.выше), но может быть и произвольной. По аналогии с произвольной формой Заявления подопечного о согласии на обработку его персональных данных.

2. Рекомендации по неотложным действиям.

Данные в в информационном сообщении JDC рекомендации целесообразно дополнить необходимостью осуществления следующих организационно-технических мероприятий:

- Разработка и утверждение внутреннего Положения, регламентирующего порядок и условия работы с персональными данными штатных сотрудников Хэсэда, персональными данными участников Хэсэда, как общественной организации и персональными данными подопечных (Положение «О работе с персональными данными»).

- Проведение масштабной работы по сбору письменных Заявлений от уже включенных в информационные базы Хэсэдов подопечных о их согласии на обработку их персональных данных и последующее получение таких согласий от вновь поступающих подопечных.

- Обращение Хэсэдов в организации, специализирующиеся на обеспечении защиты информационных систем и компьютерных баз данных, имеющие специальную лицензию, на предмет:

- точного определения категории использующихся в информационных системах и базах Хэсэда персональных данных подопечных;
- аудита защищенности существующих в Хэсэде информационных систем и компьютерных баз персональных данных подопечных и установления соответствия существующей защищенности этих систем и баз данных предъявляемым к ним требованиям с учетом категории используемых персональных данных подопечных (по содержанию), количеству подопечных, чьи данные внесены в базу;
- разработки и практической реализации рекомендаций этих организаций по обеспечению защиты информационных систем и компьютерных баз данных подопечных Хэсэда установленным требованиям.

Для классификации и защиты информационных систем персональных данных Хеседы, не располагающие необходимыми специалистами и лицензиями, могут обратиться на договорных условиях за методической и консультационной поддержкой в организации, имеющие соответствующие лицензии.

Перечень органов (организаций) по аттестации Системы сертификации средств защиты информации по требованиям безопасности информации, а также Государственный реестр сертифицированных средств защиты информации размещены на сайте ФСТЭК России: http://www.fstec.ru/_razd/_serto.htm

- Направление в территориальное управление (по месту нахождения Хэсэда) Федеральной службы по надзору в сфере связи соответствующих уведомлений *(о форме и содержании см.выше)* об осуществлении Хэсэдом обработки персональных данных для включения Хэсэда в Реестр операторов персональных данных.