Принципы защиты персональных данных

- Во-первых, это было вызвано потенциальной опасностью последствий использования по халатности или преднамеренно неточных (недостоверных), устаревших данных, их искажения или уничтожения, что представляет собой фактор качества используемых персональных данных.

- Во-вторых, скрытным (с точки зрения человека) процессом автоматизированной обработки и хранения персональных данных. Сбор многих сведений о частной жизни можно вести без ведома субъекта данных, если применять современные средства тайного наблюдения и методы расследования. Поэтому, чтобы субъект данных мог знать о сборе и хранении относящихся к нему данных, а также контролировать качество этих данных, способы и адресность их использования, были сформулированы права субъекта данных в связи со сбором, обработкой и использованием данных о нем.

Общий перечень принципов защиты данных соответствует формуле:

- принципы защиты данных = принципы качества + права субъекта данных и ограничивается 10 принципами, приведенными ниже:

- **Принципы качества. Персональные данные, проходящие автоматизированную обработку:**

1) должны быть получены на законных основаниях и обработаны добросовестным и законным способом (принцип законности данных);
2) должны накапливаться для точно определенных и законных целей и не использоваться каким-либо образом, несовместимым с этими целями (принцип законности целей);
3) должны быть адекватными, имеющими прямое отношение к делу и не быть избыточными применительно к целям, для которых они накапливаются (принцип адекватности и релевантности данных);
4) должны быть точными и, в случае необходимости, своевременно обновляемыми (принцип достоверности и актуальности данных);
5) должны храниться в форме, позволяющей идентифицировать субъектов данных только в той мере, в какой этого требуют цели, для которых эти данные накапливаются (принцип анонимности).

- **Права субъекта данных. Любому человеку должно быть предоставлено право:**

1) быть осведомленным о существовании автоматизированного файла персональных данных, о его главных целях, а также о контролере этого файла, его месте жительства, либо юридическом адресе (право на информацию о наличии собранного на индивида файла персональных данных);
2) получать через разумные интервалы времени, без излишних затрат времени и средств, как в ответ на свой запрос, так и без запроса, сообщение о том, накапливаются ли персональные данные о нем в автоматизированном файле данных (право на извещение о сборе данных);
3) получать доступ к личным персональным данным, хранимым держателем или пользователем данных (право на доступ к личным персональным данным);
4) требовать исправления или уничтожения недостоверных персональных данных, а также персональных данных, обработанных с нарушением положений национального права, реализующих принципы защиты данных (право на исправление или уничтожение недостоверных или незаконно обработанных личных данных);
5) прибегать к судебной защите нарушенного права субъекта данных (право судебной защиты).

Что касается прав субъекта данных, то они конкретизируют (применительно к сфере автоматизированной обработки данных) право индивида контролировать циркуляцию "чувствительной" информации о самом себе, столь важное для правовой защиты сферы частной жизни, что оно вошло во многие определения как "право на невмешательство в частную жизнь".

Конвенция 108 Совета Европы прямо указывает на необходимость выделения группы "высокочувствительных" данных (данные о расовом или национальном происхождении, политических взглядах, религиозных или иных убеждениях, а также данные, касающиеся здоровья, сексуальной жизни, судимости) в особую категорию данных и создания для них особого режима правовой защиты.

Ст. 7 Конвенции 108 Совета Европы обязывает стран-участниц принимать надлежащие меры для обеспечения безопасности хранящихся персональных данных от случайного или несанкционированного уничтожения или случайной утраты, а равно и от несанкционированного доступа, изменения или распространения2. Во исполнение этой статьи Конвенции большинство стран-участниц закрепило в своих национальных законах о защите данных принцип ответственности держателя и пользователя данных за принятие ненадлежащих мер обеспечения безопасности персональных данных. В этом плане самого пристального внимания заслуживает опыт Германии, где в ст. 9 специального Приложения к Федеральному закону 1990 г. о защите данных, закреплены основные организационно-технические меры обеспечения безопасности персональных данных, тем самым унифицируя их для всех субъектов федерации (федеральных земель), ведомств, отраслей и секторов экономики.

Принцип безопасности включает следующие формы защиты персональных данных:

1. принцип дифференцированной защиты;
2. принцип адресной ответственности;
3. принцип контроля доступа к устройствам обработки данных;
4. принцип контроля носителей данных;
5. принцип контроля накопителя;
6. принцип контроля пользователя;
7. принцип контроля доступа к надлежащим данным;
8. принцип контроля передачи;
9. принцип контроля ввода;
10. принцип контроля поручения;
11. принцип контроля транспортировки данных;
12. принцип организационного контроля.

Таким образом, формула состава принципов защиты данных подлежит дальнейшему расширению: принципы защиты данных = принципы качества + права субъекта данных + принцип дуализма целей + особый режим защиты "высокочувствительных" данных + принципы безопасности данных.

Спасибо за внимание !