Рекомендации для банков
по выполнению требований Регламента № 2016/679
Европейского Парламента и Совета Европейского Союза
«О защите физических лиц при обработке персональных данных и
о свободном обращении таких данных, а также об отмене
Директивы 95/46/ЕС (Общий Регламент о защите персональных данных)»,
Брюссель, 27.04.2016 (далее – Регламент)

1. Провести анализ локальных нормативных правовых актов банка на соответствие нормам Регламента

Такой анализ необходим, прежде всего, для того, чтобы установить, в каких процессах возможны нарушения по защите персональных данных в результате отсутствия соответствующих требований в ЛПНА. Кроме того, закрепление во внутренних документах, регламентирующих порядок работы, мер по исполнению норм Регламента будет являться положительным аргументом при проведении процедуры доказательства их реализации. В этой связи целесообразным является также выполнение второго пункта Рекомендаций.

2. Разработать внутренний Регламент по защите персональных данных

Его разработка будет способствовать адаптации действующих положений по защите и обработке персональных данных к требованиям Регламента с учетом специфики деятельности банка.

3. Назначить ответственное лицо по защите персональных данных

Назначение специалиста по защите данных (Data Privacy Officer) с точно определенными задачами и полномочиями повысит эффективность выполнения подразделениями банка требований по их защите. Следует провести обучение данного специалиста(-ов). Он(-и) должен(-ы) разбираться в законодательной базе и быть способным(-и) работать с обращениями граждан и надзорными органами. Также стоит учесть, что согласно Регламенту организация должна опубликовать информацию о таком сотруднике и направить ее национальному регулятору по защите персональных данных соответствующей страны Европейского Союза.

4. Провести полную инвентаризацию (учет) персональных данных клиентов – граждан ЕС, которыми располагает банк

Проведение инвентаризации поможет определить масштаб дальнейших работ, необходимых для выполнения требований Регламента на практике. Для этого требуется создать реестр всех персональных данных европейских граждан, хранимых в настоящий момент, и поддерживать его в актуальном состоянии. В реестре укажите формат персональных данных граждан ЕС (бумажный или

электронный носитель), дату и источник их получения, цель сбора/хранения и период, их значимость и т.д.

5. Провести инвентаризацию процессов, в ходе которых банк получает персональные данные граждан ЕС, и оценить данные процессы

Составьте перечень бизнес-процессов, в рамках которых происходит сбор персональных данных. Выявите процессы обработки данных, представляющих высокий риск в отношении прав и свобод их субъектов, а также трансграничные потоки персональных данных и данных, обрабатываемых с привлечением сторонних организаций.

6. Выполнить проверку процессов обработки персональных данных и набора получаемых данных с точки зрения соблюдения принципов их обработки согласно Регламенту

Принципами обработки персональных данных в соответствии с Регламентом являются:

6.1. правомерность, справедливость и прозрачность;

Определение юридической законности для обработки персональных данных особенно важно при использовании больших данных (big date) и внешних источников данных, таких как социальные сети.

Проанализируйте правомерность обработки персональных данных граждан ЕС исходя из условий, установленных пунктом 1 статьи 6 Регламента. Определите, в каких случаях требуется получение согласия владельцев персональных данных на их обработку и хранение, и обеспечьте его обязательное получение. Проверьте наличие законного основания хранения для каждого вида обработки данных.

Помните, что если обработка основывается на согласии, контролер должен быть способен подтвердить, что субъект данных согласен на обработку его/ее персональных данных. При этом согласием субъекта не будет является отсутствие действий, обратная отправка заранее заполненного вопросника, отсутствие отрицательного ответа. Также согласие считается недействительным, если для выполнения договора/предоставления услуг нет необходимости в обработке персональных данных их субъекта, а контролер тем не менее потребовал их.

6.2. целевое ограничение;

6.3. минимизация данных;

Особое внимание стоит уделить соблюдению принципа «необходимого минимума», согласно которому объем собираемых персональных данных должен соответствовать цели обработки (не следует собирать данные, которые

не требуются для достижения цели обработки). По возможности минимизируйте объем собираемых данных.

6.4. точность;

6.5. ограничение хранения;

Данный принцип означает, что персональные данные не должны храниться дольше, чем это требуется для целей обработки. Определите ожидаемый срок хранения для каждого набора персональных данных и обеспечьте их своевременное удаление.

6.6. целостность и конфиденциальность.

7. Осуществлять соответствующие технические и организационные меры, обеспечивающие надлежащий уровень безопасности данных

Проведите анализ существующих организационно-технических мер защиты информации с точки зрения требований Регламента и на постоянной основе осуществляйте мониторинг функционирования внедренных мер защиты данных. Выполните оценку рисков нарушения конфиденциальности (Data Protection Impact Assessment – DPIA) для критичных процессов обработки персональных данных.

8. Регулярно осуществляйте процедуру проверки и оценки эффективности технических и организационных мер, обеспечивающих безопасность обработки персональных данных.