ВСТРОЕННАЯ ПРИВАТНОСТЬ В IT ПРОДУКТАХ

два слова о Privacy UX

Елена Себякина

CIPP/E, Privacy by design, DPP, DPT, DPM,
CIPM trained, Senior consultant DPO LLC

ПРИНЦИПЫ GDPR

*ИСТОЧНИК: РУКОВОДСТВО **EDPB** ПО ВСТРОЕННОЙ ПРИВАТНОСТИ **4/2019***

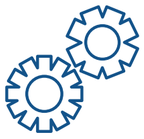
9 принципов

1	2	3	4	5	6	7	8	9
Прозрачность	Законность	Справедливость	Ограничение целью	Минимизация	Точность	Лимит срока хранения	Целостность и конфиденци-альность	Подотчетность







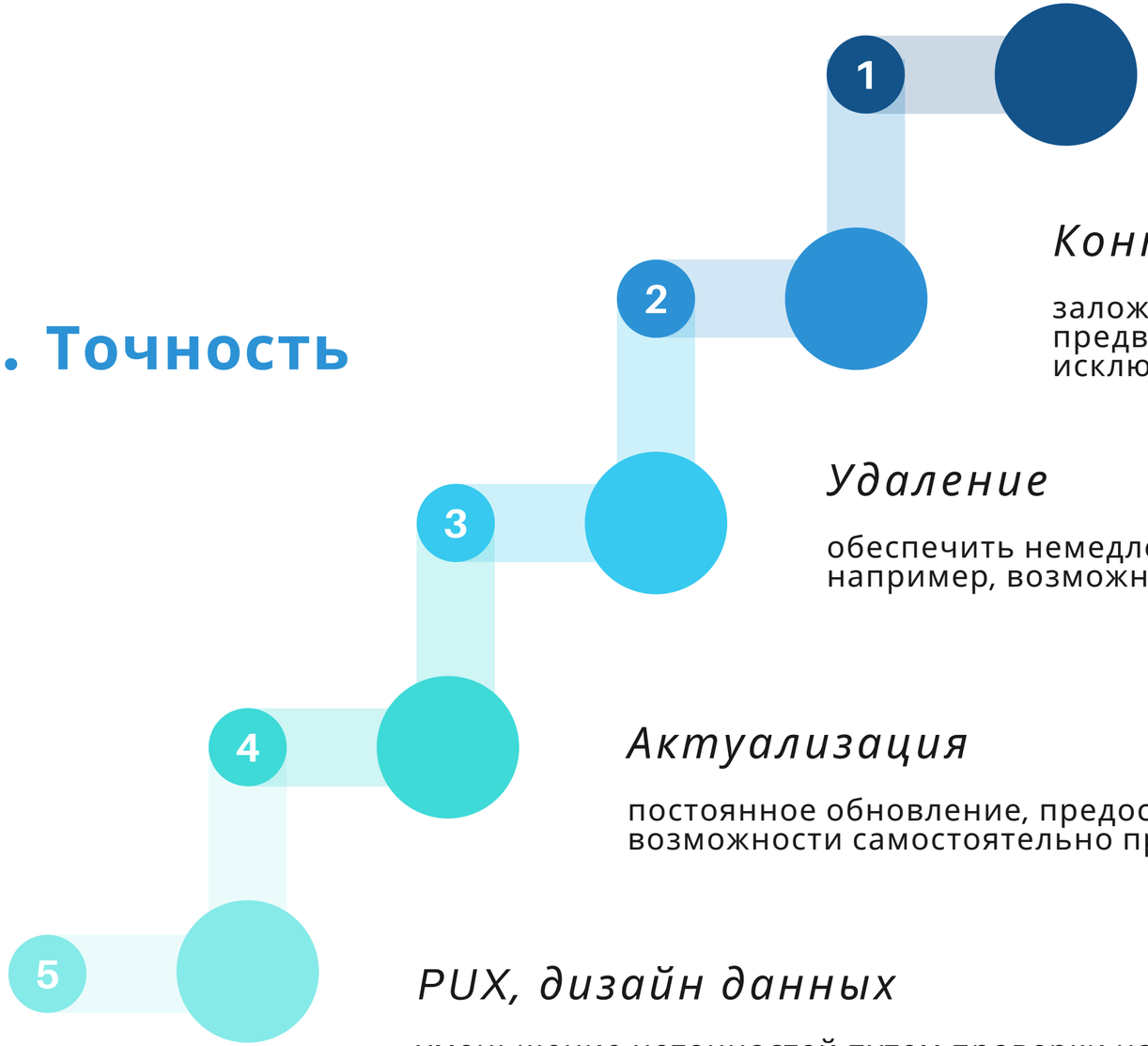




3. Справедливость

Справедливые алгоритмы	*Реализация прав*	*Соответствие ожиданиям*	*Баланс сил*	*Без манипуляций*
не позволяющие предубежденного или дискриминирующего отношения к субъектам. Рекомендуется, чтобы финальное решение принимал человек	интерфейсы должны предусматривать возможность реализовать права на приватность, коммуникации с DPO	интерфейс должен соответствовать разумным ожиданиям субъекта, не запирать его, не вымогать данные, не дискриминировать, давать автономию	не пользоваться слабостями субъекта (спешка, нужда, некомпетентность), не перекладывать риски на самого субъекта	не использовать dark patterns, манипулятивный язык или дизайн

5. Минимизация

6. Точность



Источник данных

использовать надежные источники данных

Контроль ошибок

заложить сокращение количества ложных срабатываний, предвзятости в автоматизированном принятии решений, исключить эффект накопленной ошибки

Удаление

обеспечить немедленное удаление ошибочных или устаревших данных, например, возможность удаления данных о детстве и юности субъектов

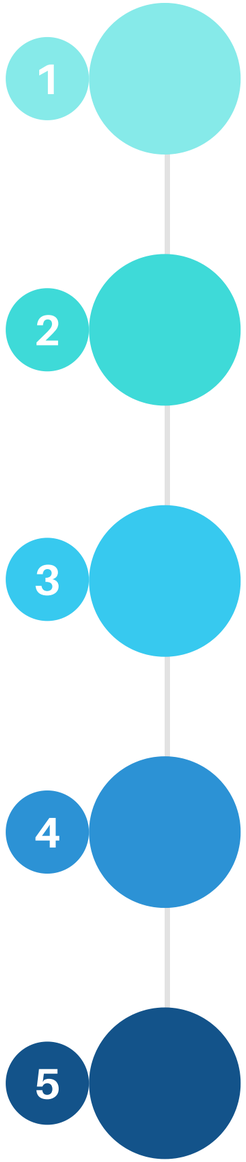
Актуализация

постоянное обновление, предоставление субъекту непосредственной возможности самостоятельно проверять, изменять, исправлять свои данные

PUX, дизайн данных

уменьшение неточностей путем проверки на всех этапах обработки, предоставления на выбор стандартных вариантов вместо полей с произвольным текстом.
Обеспечить механизмы правопреемства (наследование, смена пола и т.п.)

7. Лимит срока хранения



Удаление и анонимизация

механизмы единовременного автоматического удаления и анонимизации данных после достижения цели или срока их обработки должны быть заранее спроектированы и заложены во все системы их обработки и хранения

Эффективность

убедитесь, что повторная идентификация из анонимизированных вами данных или восстановление удаленных данных невозможны

Автоматизация

удаление должно быть автоматизировано

Критерии хранения

определите и настройте в правилах системы сроки хранения для каждой цели

Резервные копии/журналы

удаление данных должно выполняться и из резервных копий и журналов. Лимитируйте временное хранение и копирование

8. Целостность и конфиденциальность

01 *Система управления информационной безопасностью*

внедрите оперативные средства управления, политики и процедуры информационной безопасности. Проектируйте системы в соответствии с ними

02 *Анализ рисков*

периодически выполняйте прогнозирование угроз, атак, уязвимостей, проводите регулярное тестирование. Планируйте меры противодействия. Учитывайте уровень риска при выборе мер защиты данных

03 *Встраивание безопасности*

закладывайте меры безопасности при проектировании системы, при интеграции, тестировании

04 *Доступы*

спроектируйте возможность управления доступами, ограничения и разделения доступов

05 *Безопасное хранение и передача*

спроектируйте возможность безопасной передачи и хранения данных, исключающую несанкционированный и случайный доступ, изменения, возможность псевдонимизации, разделяйте базы данных, не смешивайте данные, собранные для разных целей. Спецкатегории храните отдельно. Обеспечьте безопасное резервное копирование и аварийное восстановление

Спасибо!

DPO LLC

Моя статья по встроенной приватности

Гайдлайн испанского надзорного органа по встроенной приватности

Гайдлайн французского надзорного органа по встроенной приватности