Checklist «Чи виконує ваша компанія всі вимоги GDPR? »

25 травня 2018 року набрав чинності Загальний Регламент Захисту Даних, більш відомий як GDPR (General Data Protection Regulation).

GDPR застосовується до компаній, які розташовані та здійснюють діяльність не тільки на території ЄС. Якщо ви розташовані поза межами ЄС, але ваш клієнт або компанія, таргетовані на осіб з країни ЄС і збирає персональні дані та інформацію про поведінку осіб з країни ЄС, ваша компанія підпадає під сферу дії GDPR.

Які персональні дані захищаються?

- ім'я, адреса, ідентифікаційний номер;
- дані про місцеперебування, IP-адреса, дані файлів cookie та RFID-теги;
- інформація про стан здоров'я, генетичні дані;
- номер мобільного телефону;
- номер водійського посвідчення / паспорта;
- біометричні дані;
- дані, що розкривають расову або етнічну приналежність;
- дані, що розкривають політичні переконання, релігію або філософські переконання;
- дані про статеве життя, про сексуальну орієнтацію.

Цей чекліст допоможе визначити, чи виконує ваша компанія всі вимоги GDPR, а якщо ні – виявити слабкі місця та усунути їх.

✓ **Ви оновили Політику конфіденційності та використання файлів «cookie», Умови і Правила користування веб-сайтом;**

Політика конфіденційності та використання файлів «cookie», Умови і Правила користування веб-сайтом:

- повинні бути доступними і зрозумілими, з використанням чітких і простих формулювань.
- повинні містити інформацію про ваші контактні дані, цілі опрацювання, законні підстави опрацювання персональних даних, одержувачів персональних даних, період зберігання персональних даних, або, якщо це неможливо, — критерії визначення такого періоду, існування права на запит щодо доступу до персональних даних і їх виправлення, стирання, обмеження опрацювання щодо особи або на заперечення проти опрацювання, а також права на мобільність даних; існування права на відкликання згоди тощо);
- перед тим, як надати згоду на обробку персональних даних особа повинна мати можливість ознайомитись з цими документами (напр. перейти за гіперпосиланням).

✓ **Ви отримуєте згоду на обробку персональних даних згідно з Регламентом;**

Згоду необхідно надавати шляхом чіткого ствердження, що становить вільно надане, конкретне, проінформоване та однозначне свідчення погодження особи на опрацювання персональних даних. Згода на обробку персональних даних - це, наприклад, заповнення клітинки позначкою під час відвідування веб-сайту в мережі Інтернет, обрання технічних налаштувань для послуг інформаційного суспільства або інша заява чи поведінка, що чітко вказують на погодження особою із запропонованим опрацюванням персональних даних.

Автоматичне заповнення клітинок позначками, інші методи отримування згоди за замовчуванням, мовчання, або бездіяльність не становлять надання згоди. Згода не є дійсною:

- якщо заява про надання згоди не містить чітких і простих формулювань;
- якщо в особи не має можливості відмовити в наданні згоди або її відкликати, не заподіюючи при цьому шкоди;
- якщо особу не поінформовано про цілі опрацювання персональних даних.

✓ **Ви зберігаєте записи щодо опрацювання персональних даних;**

Щоб довести відповідність Регламенту, ви повинні зберігати записи щодо опрацювання даних, а у випадку надходження запиту від наглядового органу, надати йому такі записи. У випадку перевірки ви повинні могти продемонструвати, коли саме і як саме особа надала згоду на обробку персональних даних.

✓ **Ви забезпечуєте умови для подання та реагування на запити щодо персональних даних;**

- Ви уможливили подачу запитів щодо персональних даних у електронному форматі (шляхом заповнення форми на веб-сайті, надсилання email тощо);
- Ви готові відповідати на запити щодо персональних даних протягом одного місяця;

Якщо особа звертається із запитом про надання інформації — повідомити, чи обробляються дані стосовно запитувача, які категорії персональних даних опрацьовуються, цілі, для яких опрацьовують персональні дані; за можливості, період, протягом якого опрацьовують персональні дані, або, якщо це неможливо, — критерії визначення такого періоду; одержувачів персональних даних;

Якщо особа звертається із запитом про отримання копії персональних даних — надати копію персональних даних (перший раз безкоштовно, у разі подальших звернень можна стягувати розумну плату, що ґрунтується на адміністративних витратах);

Якщо особа звертається про передання своїх персональних даних іншій компанії — надати їх в структурованому, загальноприйнятому форматі, що легко зчитується машиною, якщо опрацювання персональних даних є автоматизованим. Наприклад, особа, яка використовує додаток Strava для відстеження фізичної активності, хоче змінити його на Runkeeper. Вона може звернутися за імпортом своїх даних в Runkeeper. Таким чином забезпечується мобільність даних всередині ЄС.

Якщо особа звертається із запитом про виправлення неточних персональних даних — виправити такі персональні дані без затримки, а також повідомити кожного одержувача, якому було розкрито персональні дані;

Особа може в будь-який момент відкликати згоду або заперечити проти опрацювання своїх персональних даних. Крім цього, Регламент дозволяє звертатись до пошукових сервісів із вимогою видалити посилання на інформацію, яка містить персональні дані особи. У разі надходження такого запиту, Ви повинні видалити персональні дані та повідомити кожного одержувача, якому було розкрито персональні дані. Щоправда, із цього правила є винятки, коли, наприклад, інформація необхідна для забезпечення права на свободу вияву поглядів та свободу інформації, громадського здоров'я, наукової, історичної чи статистичної мети, вирішення юридичних спорів.

✓ **Контрагенти, яким передаються персональні дані, повинні дотримуватися GDPR**

Якщо ви передаєте персональні дані контрагентам для опрацювання, ви відповідаєте за те, щоб їхня діяльність відповідала вимогам GDPR. У випадку виявлення порушень зі сторони контрагентів, до вас також можуть бути застосовані штрафні санкції. Тому, відносини щодо опрацювання персональних даних необхідно регулювати договором.

✓ **Ви забезпечуєте технічні заходи безпеки персональних даних;**

Технічні заходи безпеки повинні забезпечувати високий рівень безпеки інформації. Вони можуть бути досить різноманітними. Це залежить від того, які саме дані обробляються, від їхньої кількості, можливості витоку, викрадення тощо. Як приклад заходів, які можуть застосовуватися, Регламент наводить використання псевдонімів і шифрування.

✓ **Ви видаляєте персональні дані:**

- якщо вони більше не є потрібними щодо цілей, для яких їх збирають або іншим чином опрацьовують;
- строк зберігання яких закінчився;
- якщо особа відкликала згоду або заперечує проти подальшого опрацювання.

- ✓ **Ви повідомляєте про витік персональних даних;**

Якщо витік персональних даних є значним, Ви повинні протягом 72 годин повідомити особу, якій належать персональні дані та наглядовий орган. Особу, якій належать персональні дані, можна не повідомляти, лише якщо було вжито необхідних технічних та організаційних заходів захисту, або повідомлення передбачатиме докладання надмірних зусиль. Тому, наприклад, компанія Uber, яка приховала витік даних 57 млн. користувачів, вважалася би порушником GDPR. Якби інцидент стався не у 2016 році, а після набрання чинності GDPR, компанії загрожував би значний штраф.