

Защита персональных данных сотрудников (GDPR)

Igor Kyrzewski · 24.05.2025 · Kadry i Płace – JDG, Kadry i Płace – Spółki

▣ Введение

Каждый работодатель обрабатывает персональные данные своих сотрудников – начиная с момента найма, на протяжении всего периода работы, до хранения документации после его завершения. Эти принципы регулируются:

- Регламентом Европейского парламента и Совета (ЕС) 2016/679 (GDPR),
- Трудовым кодексом, и
- Законом о защите персональных данных от 10 мая 2018 года

▣ 1. Какие персональные данные может обрабатывать работодатель?

▣ Обязательные данные (на основании ст. 22¹ Трудового кодекса):

- Найм - имя, фамилия, контактные данные, образование, опыт работы
- Трудоустройство - PESEL, адрес, данные детей (для налоговых целей), номер банковского счета
- В период трудоустройства - данные о инвалидности, медицинские справки, судебные акты (если требуется)
- После окончания трудовой деятельности - данные в личных делах в течение 10 лет

▣ Биометрические, генетические, медицинские или религиозные данные не могут быть **обработаны** работодателем, если это не требуется законом и не

является необходимым.

▣ 2. Обязанности работодателя как администратора данных

Согласно GDPR работодатель как администратор данных обязан:

▣ а) Законность обработки

- Данные могут обрабатываться **на основании трудового контракта** или **юридического обязательства** (например, Трудового кодекса, Социального страхования, Налогового управления) – согласие не требуется

▣ б) Сокращение данных

- Только данные **необходимые для цели** (например, трудоустройство, расчет зарплаты, Социальное страхование)

▣ с) Предоставление информационной оговорки

- Обязанность по информированию – например, во время найма и трудоустройства (ст. 13 и 14 GDPR),
- Должны включать: администратора, цель, юридическую основу, срок хранения, права работника.

▣ d) Безопасность данных

- Организационные (например, доступ только для HR-отдела),
- Технические (пароли, шифрование, контроль доступа).

▣ e) Хранение данных только столько, сколько необходимо

- Персональные данные в личных делах – **10 лет**,
- Данные, обрабатываемые на основании согласия – **до отзыва или выполнения цели**.

□ 3. Информационные обязательства перед работником

Работник должен быть информирован, в числе прочего, о:

- цели и объеме обработки данных,
- его правах (доступ, исправление, возражение, удаление, ограничение),
- контактных данных уполномоченного по защите данных (если назначен),
- праве на подачу жалобы Президенту Управления по защите персональных данных.

□ Информация должна предоставляться **в письменной или электронной форме** (например, в качестве приложения к контракту или регламентам).

□ 4. Права работника (как субъекта данных)

- Доступ к данным - Право просматривать и получать копию данных
- Исправление данных - Возможность запросить исправление некорректных данных
- Удаление ("право быть забытым") - Только когда данные обрабатываются на основании согласия
- Ограничение обработки - В определенных ситуациях (например, спор в отношении точности данных)
- Возражение - Когда данные обрабатываются на основании законного интереса

□ На практике данные, возникающие в рамках **Трудового кодекса и публичных юридических обязательств**, не могут быть удалены по запросу (например, личные дела, документы для Социального страхования).

□ 5. Могут ли обрабатываться данные кандидатов, семьи, здоровья?

- Данные кандидатов на работу - Только необходимые (ст. 22¹ Трудового кодекса) + согласие на CV
- Данные о детях (для пособий, Фонд социальных пособий) - Да, но только если это требуется законом (например, PIT-2)
- Данные о здоровье - Только на основании направления к врачу / судебного акта
- Фотографии, мониторинг, местоположение - Необходимая информация и обоснование в регламентах

▣ 6. Последствия нарушения GDPR

Отсутствие информационной оговорки - Жалоба в Управление по защите данных, рекомендации, предписание об удалении данных

Обработка ненужных данных - Предупреждение или административный штраф

Потеря или раскрытие данных - Штраф до 20 миллионов евро или 4% от оборота (на практике: до 1 миллиона PLN в Польше)

Неисполнение обязанности о сообщении о нарушении - Дополнительные санкции и проверки

▣ Юридическая база

- **GDPR** (Регламент Европейского парламента и Совета (ЕС) 2016/679),
- **Трудовой кодекс** – ст. 22¹–22⁵
- **Закон от 10 мая 2018 года о защите персональных данных**