Защита персональных данных

Ваше имя – это часть персональных данных, нуждающихся в защите.

Каждый имеет право на:

пользование именем;

неприкосновенность имени;

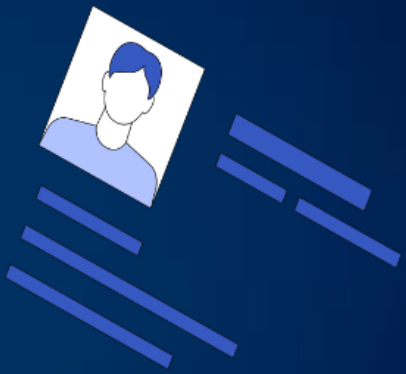
перемену имени;

защиту имени.

Вред, причиненный гражданину в результате неправомерного использования его имени, подлежит возмещению в соответствии с Гражданским Кодексом РФ.

Статья 58 Семейного кодекса РФ, статьи 19, 1198, 1265 Гражданского кодекса РФ.

Что еще относится к персональным данным?



фамилия, имя и отчество человека;
пол; дата и место рождения;
уровень образования; место жительства;
семейное положение; номер телефона;
адрес электронной почты;
место работы и занимаемая должность работника;
уровень доходов.

Также к персональным данным относится и фотография человека, с помощью которой возможно установить личность.

Почему важно обеспечивать сохранность персональных данных?

• Финансовые последствия

Мошенник может получить полный доступ к банковским счетам или кредитным картам, сможет совершать транзакции от вашего имени. Он использует методы социальной инженерии, чтобы выведать дополнительную информацию (кодовые слова, логин и пароль от приложения, коды из СМС-уведомлений и т.д.).

• Угроза конфиденциальности

В результате кражи персональных данных злоумышленник может получить доступ к личным сообщениям, контактной и другой конфиденциальной информации. Впоследствии ее могут использовать для шантажа, спам-рассылок или просто для нанесения репутационного ущерба. Это может негативно повлиять на личную и профессиональную жизнь человека.

@cyberpolice_rus

Обработка персональных данных без вашего согласия - незаконна

Тот факт, что человек дал согласие на обработку своих персональных данных оператору, к примеру, социальной сети, который разместил их на своем ресурсе, не дает право иным операторам использовать персональные данные этого человека.

По общему правилу, обработка персональных данных субъекта осуществляется на основании согласия, однако есть случаи, когда обработка персональных данных осуществляется без согласия субъекта персональных данных (пп. 2-11 ч. 1 ст. 6; пп. 2-10 ч. 2 ст. 10; ч. 2 ст. 11 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

@cyberpolice_rus

Гражданин имеет право:

- Свободно давать согласие на обработку персональных данных.

- Отозвать согласие на обработку персональных данных.

- Получать информацию о своих персональных данных.

- Требовать от операторов уточнить, блокировать или уничтожить персональные данные.

- Обжаловать действие или бездействие оператора, требовать устранения нарушения, компенсации ущерба.

Как удалить персональные данные из открытого доступа?

Чтобы удалить персональные данные с сайта, нужно подготовить требование к его владельцу.

Требование должно содержать: фамилию, имя, отчество (при наличии), вашу контактную информацию и перечень персональных данных, которые нужно удалить с сайта.

С момента поступления требования оператор обязан прекратить распространение данных в течение 3 рабочих дней.

В случае отказа вы можете обратиться в Центр правовой помощи гражданам в цифровой среде. Они помогут Вам составить жалобу в Роскомнадзор или иск в суд.

Как удалить персональные данные из открытого доступа?

Из поисковой системы можно удалить ссылки на сведения, которые, по мнению человека, могут нанести ему вред, устаревшие, неуместные, неполные, неточные или избыточные данные, а также информацию, законные основания для хранения которой исчезли с течением времени.

Чтобы удалить данные:

Подготовьте списки ссылок, содержащих недостоверную информацию, документы, удостоверяющие личность, и доказательства вашей позиции: подтверждение недостоверности или неактуальности данных, опровержение материалов, порочащих репутацию компании, или решение суда о клевете. Обратитесь в службу поддержки поисковой системы и передайте собранную информацию.

Базовые принципы обеспечения сохранности персональных данных

Чтобы сохранить данные необходимо:

не передавать персональные данные подозрительным операторам;

начать периодически менять пароли;

сделать отдельную почту для сомнительных сайтов;

обращать внимание на ссылки и адреса сайтов во избежание фишинга;

пользоваться персональными средствами защиты информации;

обновлять программы и операционную систему.