ПОВІДОМЛЕННЯ ПРО ПОРУШЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Шановна пані / Шановний пане,

З жалем повідомляємо вам, що стався інцидент, в результаті якого неуповноважені особи могли отримати доступ до ваших персональних даних. Ці дані зберігалися та використовувалися компанією Flexidea sp. z o. o. з місцезнаходженням в Лодзі. Цю компанію придбала компанія Contrain Poland sp. z o. o. з місцезнаходженням в Лодзі (далі – «Адміністратор даних»), тому ми несемо відповідальність за інформування вас про цей інцидент та вжиття відповідних заходів.

Проблема виникла в системі зовнішньої компанії, яка займалася бухгалтерським обліком Flexidea sp. z o. o. та надавала систему для виставлення та зберігання рахунків-фактур.

У наступному розділі ми пояснюємо, що сталося, якими можуть бути наслідки, що ми зробили з цього приводу та як ви можете захистити свої дані від неправомірного використання.

1. **Що сталося?**
   27–28 вересня 2026 року відбулася хакерська атака на IT-системи компанії, яка надає бухгалтерські послуги та забезпечує платформу для виставлення та зберігання рахунків-фактур, якою користувалася компанія Flexidea sp. z o. o. В результаті атаки неуповноважена особа отримала доступ до системи та скопіювала деякі дані, що зберігаються в ній, включаючи ваші персональні дані.
   Інцидент призвів до порушення захисту конфіденційності персональних даних. Однак не було жодних доказів того, що дані були змінені, видалені або стали недоступними в результаті цього.

2. **Які ваші персональні дані постраждали від витоку інформації?**
   З наявної у нас інформації випливає, що порушення могло стосуватися таких Ваших персональних даних:
   - ім'я та прізвище;
   - серія/ номер паспорта;
   - адреса проживання.

3. **Які можуть бути наслідки порушення та що ви можете зробити?**
   Розкриті дані можуть бути використані неуповноваженими особами, зокрема, для спроб видати себе за вас, отримати додаткові персональні дані або вдатися до шахрайства, зокрема через електронні листи, телефонні дзвінки чи кореспонденцію, надіслану на вашу домашню адресу. Не можна також повністю виключити спроб використати ці дані для перевірки особи або надання послуг, якщо заходи безпеки, що застосовуються організацією, виявляться недостатніми.

Щоб зменшити ризик, ми рекомендуємо:

- будьте особливо обережні під час отримання повідомлень, телефонних дзвінків або інших спроб зв’язатися з вами, особливо коли особа, яка зв’язується з вами, стверджує, що знає ваші персональні дані, номер паспорта чи домашню адресу;
- не надавайте скановану копію або фотографію паспорта чи додаткові персональні дані, паролі, одноразові коди чи банківську інформацію без попередньої перевірки особи та достовірності одержувача;
- звертайте увагу на незвичайне листування, зокрема інформацію, що стосується невідомих вам договорів, зобов'язань, вимог про оплату або спроб підтвердити вашу особу;
- у разі сумнівів зверніться до органу, який видав паспорт, або до відповідного консульського відділу, щоб з'ясувати, чи рекомендуються додаткові заходи безпеки;
- у разі підозри щодо несанкціонованого використання даних негайно зверніться до відповідної установи, а у разі підозри у скоєнні злочину – повідомте відповідні правоохоронні органи.

Саме розголошення номера вашого паспорта не означає, що вам потрібно замінити документ. Будь-які дії, які ви вживаєте в цьому відношенні, повинні бути узгоджені з відповідним органом країни, яка видала паспорт.

Наразі ми не маємо інформації, яка б свідчила про використання ваших даних неуповноваженими сторонами. Однак такий ризик не можна виключати в майбутньому.

4. **Які заходи були вжиті у відповідь на порушення?**
   Після виявлення інциденту, компанія, яка керує платформою виставлення рахунків, вжила заходів для захисту системи та запобігання подальшому несанкціонованому доступу. Це включало, зокрема, блокування несанкціонованого доступу, усунення використаної вразливості безпеки, зміну даних доступу та перенесення платформи на нове серверне середовище. Вразливість безпеки була усунена 28 вересня 2026 року. Про інцидент також повідомлено до CERT Polska та поліції.
   Як правонаступник компанії Flexidea sp. z o. o., ми проаналізували обсяг даних, що охоплюються порушенням, та пов'язані з цим ризики, повідомили про порушення Голові Управління захисту персональних даних та вжили заходів для інформування осіб, чиї права чи свободи можуть опинитися під високим ризиком внаслідок порушення. Ми також постійно контактуємо з компанією, яка керує платформою виставлення рахунків, щоб отримати додаткову інформацію щодо інциденту та будь-яких додаткових ризиків, пов'язаних з розкритими даними.

5. **Де можна отримати додаткову інформацію?**
   Якщо у вас виникли будь-які запитання щодо порушення захисту персональних даних, його можливих наслідків або рекомендованих запобіжних заходів, зверніться до інспектора із захисту даних, пана Адама Копа, електронною поштою iod@contrain.pl або

письмово на адресу Contrain Poland sp. z o. o., ul. 3 Maja 14a, 93-408 Łódź, з позначкою «Inspektor Ochrony Danych».

Вибачте за цю ситуацію та незручності, які вона може спричинити. Запевняємо вас, що ми відповідально ставимося до захисту персональних даних та вживаємо заходів для зменшення наслідків порушення.

З повагою,
Contrain Poland sp. z o.o.
ul. 3 Maja 14a
93-408 Łódź

СООБЩЕНИЕ О НАРУШЕНИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Уважаемая госпожа / Уважаемый господин,

С сожалением сообщаем вам, что произошел инцидент, в результате которого неуполномоченные лица могли получить доступ к вашим персональным данным. Эти данные хранились и использовались компанией Flexidea sp. z o. o. с местонахождением в Лодзи. Эту компанию приобрела компания Contrain Poland sp. z o. o. с местонахождением в Лодзи (далее – «Администратор данных»), поэтому мы несем ответственность за информирование вас об этом инциденте и принятии соответствующих мер.

Проблема возникла в системе внешней компании, которая занималась бухгалтерским учетом Flexidea sp. z o. o. и предоставляла систему для выставления и хранения счетов-фактур.

В следующем разделе мы объясняем, что случилось, какими могут быть последствия, что мы сделали в связи с этим и как вы можете защитить свои данные от неправомерного использования.

1. **Что произошло?**
   27–28 сентября 2026 г. произошла хакерская атака на ИТ-системы компании, предоставляющей бухгалтерские услуги и обеспечивающей платформу для выставления и хранения счетов-фактур, которой пользовалась компания Flexidea sp. z o. o. В результате атаки неуполномоченное лицо получило доступ к системе и скопировало некоторые данные, хранящиеся в ней, включая ваши персональные данные.
   Инцидент привел к нарушению защиты конфиденциальности персональных данных. Однако не было никаких доказательств того, что данные были изменены, удалены или стали недоступны в результате этого.

2. **Какие ваши персональные данные пострадали от утечки информации?**
   Согласно имеющейся у нас информации, была нарушена защита таких ваших персональных данных:
   - имя и фамилия;
   - серия/ номер паспорта;
   - домашний адрес.

3. **Какие могут быть последствия нарушения и что вы можете сделать?**
   Раскрытые данные могут быть использованы неуполномоченными лицами, в частности, для попыток выдать себя за вас, получить дополнительные персональные данные или прибегнуть к мошенничеству, в частности, через электронные письма, телефонные звонки или корреспонденцию, высланную на ваш адрес. Нельзя также полностью исключить попытки использовать эти данные для проверки личности или

предоставления услуг, если меры безопасности, применяемые организацией, окажутся недостаточными.

Чтобы уменьшить риск, мы рекомендуем:

- будьте особенно осторожны при получении сообщений, телефонных звонков или других попыток связаться с вами, особенно когда лицо, связывающееся с вами, утверждает, что знает ваши персональные данные, номер паспорта или домашний адрес;
- не предоставляйте сканированную копию или фотографию паспорта или дополнительные персональные данные, пароли, одноразовые коды или банковскую информацию без предварительной проверки личности и достоверности получателя;
- обращайте внимание на необычную переписку, в частности информацию, касающуюся неизвестных вам договоров, обязательств, требований об оплате или попыток подтвердить вашу личность;
- в случае сомнений обратитесь в орган, выдавший паспорт или в соответствующий консульский отдел, чтобы выяснить, рекомендуются ли дополнительные меры безопасности;
- в случае подозрения в несанкционированном использовании данных немедленно обратитесь в соответствующее учреждение, а в случае подозрения в совершении преступления – проинформируйте соответствующие правоохранительные органы.

Само разглашение номера вашего паспорта не означает, что вам нужно заменить документ. Любые действия, которые вы предпринимаете в этом отношении, должны быть согласованы с соответствующим органом страны, выдавшей паспорт.

Сейчас мы не располагаем информацией, свидетельствующей об использовании ваших данных неуполномоченными лицами. Однако такой риск нельзя исключать в будущем.

4. **Какие меры были предприняты в ответ на нарушения?**

После обнаружения инцидента компания, управляющая платформой выставления счетов, приняла меры для защиты системы и предотвращения дальнейшего несанкционированного доступа. Они включали, в частности, блокировку несанкционированного доступа, устранение использованной уязвимости безопасности, изменение данных доступа и перенос платформы на новую серверную среду. Уязвимость безопасности была устранена 28 сентября 2026 года. Об инциденте также сообщено CERT Polska и полиции.

Как правопреемник компании Flexidea sp. z o. o., мы проанализировали объем данных, охватываемых нарушением, и связанные с этим риски, сообщили о нарушении Председателю Управления по защите персональных данных и приняли меры по информированию лиц, чьи права или свободы могут оказаться под высоким риском вследствие нарушения. Мы также постоянно контактируем с компанией, управляющей

платформой выставления счетов, чтобы получить дополнительную информацию об инциденте и любых дополнительных рисках, связанных с раскрытыми данными.

5. **Где можно получить дополнительную информацию?**
   Если у вас возникли какие-либо вопросы о нарушении защиты персональных данных, его возможных последствиях или рекомендованных мерах, обратитесь к инспектору по защите данных, господину Адаму Копу, по электронной почте iod@contrain.pl или в письменном виде по адресу Contrain Poland sp. z o.o., ul. 3 Maja 14a, 93-408 Łódź, с пометкой «Inspektor Ochrony Danych».

Просим прощения за эту ситуацию и неудобства, которые она может вызвать. Уверяем вас, что мы ответственно относимся к защите персональных данных и принимаем меры по уменьшению последствий нарушения.

С уважением,
Contrain Poland sp. z o.o.
ul. 3 Maja 14a
93-408 Łódź