



Kreisverwaltung



Kreisverwaltung Rhein-Pfalz-Kreis, Postfach 21 72 55, 67072 Ludwigshafen

Distributors:

Official gazettes RPK, FT, LU, SP

Official gazettes of the district municipalities

Daily newspapers (Die Rheinpfalz, Mannheimer Morgen, Rhein-Neckar-Zeitung)

Notice

(Foreign-language) notice of publication on RPK homepage
(there also in the following languages: German, English, French, Ukrainian, Arabic, Turkish, ...)

Responsible Office

Name

Room

Phone

Fax

E-mail

Our reference

Your reference

Your message from

Date

District Administrator's Office

Clemens Körner

A 300

24.11.2022

Notification of data subjects about the violation of the protection of personal data pursuant to §§ 54 et seq. Rhineland-Palatinate State Data Protection Act (LDSG) and/or Art. 33 et seq. General Data Protection Regulation (GDPR)

Public notice pursuant to § 55 (3) no. 3 LDSG, Art. 34 (3) lit. c GDPR

Legal basis	Keyword	Concrete information
§ 55 (2) LDSG Art. 34 (2) GDPR	Type of violation of the protection of personal data	By using a so-called "ransomware", (personal) data on the district's servers was encrypted so that access is no longer possible. The data stored on the servers was stolen to a small extent, and in the meantime the criminal perpetrators have published data on the Darknet. The data can be called up and viewed there.
§ 54 (3) no. 2 LDSG Art. 33 (3) lit. b GDPR	Name of the official data protection officer and/or information office	Data Protection Officer of the Rhein-Pfalz District Administration Mr Thomas Hauck Europaplatz 5 67063 Ludwigshafen

Office address
District administration
Rhein-Pfalz
Europaplatz 5
67063 Ludwigshafen

Contact
Phone 0621 5909-0

www.rhein-pfalz-kreis.de

Bank details
Sparkasse Vorderpfalz IBAN DE39 5455 0010 0000 0114 29 BIC LUHSDE6AXXX
VAT ID No. : DE 149137931

Legal basis	Keyword	Concrete information
§ 54 (3) no. 3 LDSG Art. 33 (3) lit. c GDPR	Description of the likely consequences of the violation	The type of breach described has caused personal data to be criminally stolen and published. The data is accessible and can be used by third parties. It is not possible to delete this data. At present, it cannot be ruled out that the data will be used for criminal purposes. We ask that the instructions listed in the explanatory statement be observed with immediate effect.
§ 54 (3) no. 4 LDSG Art. 33 (3) lit. d GDPR	Description of measures taken and/or envisaged to remedy the breach or mitigate adverse effects	The hacker attack constitutes a criminal offence, which results in corresponding investigations. These have not yet been completed. In the further course of the investigation, the district administration will try to determine the course of events and, depending on the outcome, take further steps to ensure future data security. Concrete measures cannot be named at this time because the proceedings have not yet been concluded.

Reasons:

The Rhein-Pfalz district administration was the victim of a hacker attack on its computer network at the end of October 2022.

Through the use of so-called "ransomware", data on the district's servers was encrypted so that access is no longer possible. In addition, data was stolen from the servers. In the meantime, the criminal perpetrators have published a significant amount of data on the Darknet. The data can be called up and viewed there.

This process is not unique in its breadth and depth, both in the public administration sector as well as in industry. Nevertheless, we are severely restricted in our ability to work. We inform you about the possibilities to clarify your concerns on the homepage of the district at <https://www.rhein-pfalz-kreis.de/stoerung/?sds=1>

However, what is crucial and also more than regrettable is that we currently must assume that the protection of personal data could not be guaranteed to the extent that we would like and that it is also our technical and organisational expectation.

We are confidently working together with all the agencies involved in order to shed light on this criminal act on the one hand, and on the other hand to ensure the adequate protection of all data now and in the future.

The district administration has no control over what might happen to the stolen data in terms of misuse. Therefore, since we cannot be sure that the published data won't be used by third parties, we generally ask you to take the following measures:

- Change passwords (business and private).
- Check account transactions regularly.
- Keep the anti-virus programme on the private PC and updates of the operating system up to date. Activate the firewall there as well.

- Be vigilant when
- your bank reports suspicious credit card payments.
- your contacts notice that spam is being sent from your address.
- logins do not work, even though the data is correct.
- devices such as PCs, laptops or mobile phones use greatly more battery power.

Further information can be found at the consumer advice centre at <https://www.verbraucherzentrale.de/wissen/digitale-welt/apps-und-software/schadprogramme-which-gives-you-what-you-do-how-you-protect-yourself-68892>

This notice constitutes information pursuant to LDSG. We reserve the right to issue further notices depending on further developments.

We reserve the right to provide further information to individual data subjects.

Ludwigshafen, 24. November 2022

Clemens Körner
District Administrator

NOTE:

The full text of the public notice can also be found at <https://www.rhein-pfalz-kreis.de/stoerung/benachrichtigung-nach-dsgvo/>