Jens Engelhardt, attorney-at-law
specialist attorney for IT law
specialist attorney for IP law
specialist attorney for Copyright and media law

Erdem Durmus LL.M., CIPP/E

NOTOS Xperts GmbH
Heidelberger Str. 6
64283 Darmstadt
Tel.: +49 6151 520 10 0
info@notos-xperts.de

Data transfer by fax

Decision of the higher administrative court of Lower Saxony (OVG) - 11 LA 104/19

With its decision of the 22nd of July, the higher administrative court of Lower Saxony (OVG) emphasized the importance of fax transmission and data protection. In the action for a declaratory judgment, the plaintiff requested to know whether the transmission of a notice containing personal data by the authority by fax was unlawful.

In the present case the court ruled as follows:

> "When transmitting personal data by fax, the authority must take precautionary measures to guarantee the basic right to informational self-determination of the data subject. The level of protection to be maintained depends on the sensitivity and significance of the data to be transmitted, the potential risks involved in fax transmission, the degree to which the data subject is in need of protection, and the effort involved in the security measures."
>
> *"In view of the special need for protection of the plaintiff and his personal data, an increased level of protection must be maintained during the processing of the data in question with the aid of a data processing system. An unencrypted transmission of the*

plaintiff's personal data by fax falls below the level of protection to be observed. The Administrative Court rightly points out that there is no obstacle to the unauthorized perception of the data in the case of transmission by fax."[1]

Data security for telefax traffic

Most fax machines use the telephone network to send information. This type of transmission can be compared to sending a postcard, after which anyone can view the information. For this reason, it is particularly important to use the appropriate technical and organizational measures when sending personal data, in order to guarantee a secure data transfer.

Sometimes it is also human error, such as typos or transposed numbers, which can cause personal data to fall into the wrong hands.

Risks of telefax traffic

The risks of fax traffic result from a lack of data security measures. The basis of fax traffic based on the telephone network and limited fax machine equipment reveals the great weakness of this information transfer. Like a telephone conversation, information is generally transmitted unencrypted and does not use any other security measures that prevent third parties from accessing, changing, or deleting the information. A further characteristic of fax traffic is the addressing and its susceptibility to misdirection due to typing errors. Addressing by a sequence of numbers or the fax number, in contrast to multiple addresses or e-mail addresses, opens an increased risk of human error.

Fax machines are another risk. These usually do not have any password and authentication measures for incoming faxes and thus allow open access to personal data. It is therefore possible that unauthorized persons can print out the incoming fax documents without control. Furthermore, it cannot be guaranteed that the receiving system also uses a fax machine. If this is not the case, the documents are usually forwarded to a specific e-mail box or e-mail distribution list.

Some newer fax machines also have a remote maintenance function, which can pose a security risk under certain circumstances. The remote maintenance function allows access to the stored data without the owner's knowledge. Another problem can be call detour, whereby fax machines are temporarily switched to other connections and thus pose a risk to the personal data sent.

[1] https://openjur.de/u/2263419.html.

Principles and measures for handling faxes in accordance with data protection regulations

Fax traffic is very similar to telephone traffic due to the use of the same network, which means that its use can be considered the same under data protection law. The controller must therefore check whether sending data worthy of protection by fax is necessary and appropriate. A transmission, especially of sensitive personal data, should only be carried out in exceptional cases and under detailed security measures. It should be checked whether the document must reach the recipient directly or whether it can also be delivered via third parties. Finally, reasonable care should be taken when entering the destination numbers and using the fax machine in general.[2]

Within the scope of technical and organizational measures, care must be taken to ensure that the fax machines are set up in such a way that no unauthorized persons can gain knowledge of the content of the information. Furthermore, the fax machines should only be operated by the responsible personnel. In the case of sensitive data, an exact time of transmission and the receiving device should be coordinated with the recipient in order to prevent third parties from interfering. These arrangements protect above all against misdirections, outdated connection numbers or call detour.

In order to maintain the secrecy of telecommunications, the documentation obligations must also be observed, whereby meaningful blanks and transmission/reception protocols should be kept and filed confidentially.

Many new fax machines already offer security measures to protect the transmission of personal data and should also be used. These include, for example, indication of trouble-free transmission, secure intermediate storage, retrieval by password and blocking of the remote maintenance option. It should also be ensured that all stored data is deleted after final use of the device. Intermediate storage of regularly used fax or destination numbers can also reduce faulty transmissions. It is also possible to use certain additional components on the fax machine to encrypt the information sent. Decryption is then only possible at the legitimate recipient. However, this requires that the recipient has the appropriate components. It is therefore necessary that both sender and recipient have the components for encrypting the documents. Finally, a cover page of the fax should contain information about the sender, the exact address of the recipient and the pages transmitted.

[2] https://www.datenschutz-bayern.de/technik/orient/telefax.htm.

In summary, the following must be considered when using the fax in accordance with data protection laws:

- Check the necessity and appropriateness of sending by fax
- Observe external organizational measures for using the fax machine
- Use internal technical security measures of the fax machine
- Use encryption mechanisms if necessary

We consult you in all data protection questions and provide an external data protection officer for you. Feel free to contact us!

Kind regards, the NOTOS Xperts Team!