[redacted]

[redacted]

[redacted]

Legal Department

by IMI A60FD

Date: **25. September 2020**

[redacted]

Final Decision – Complaint against [redacted]
- IMI [redacted]
- IMI Case Register entry [redacted]
- IMI Draft-Decision [redacted]
- IMI Revised Draft Decision [redacted]

Dear colleagues,

in the following, you can find the final decision. As no objections were raised, there are no changes to the previous revised draft decision.

Yours sincerely,

[redacted]

[redacted]

Administrative Fine

(Final Decision)

Dear Mr. [redacted],

according to our findings, persons entitled to act on behalf of [redacted] represented by you have committed the following administrative offence, for which [redacted] is responsible:

The [redacted] is contractual partner for all (registered) users of the [redacted] In this respect, it is responsible under data protection law for providing information in accordance with Art. 15 (1) General Data Protection Regulation (GDPR) to those users who make a corresponding application.

The original process of providing information by [redacted] to requesting users of the websites [redacted] was carried out in the manner described below:

When persons contacted the company via a communication channel provided by [redacted] and requested information pursuant to Art. 15 (1) GDPR, they received an e-mail from the internally responsible customer service department of [redacted] to which a password-encrypted document containing the requested information was attached (content-encrypted e-mail). The information could contain, among other things, account information of the respective requesting user (e.g. first name, surname, e-mail address, address, telephone number, currency data), a copy of an identity card, PayPal data, [redacted]. A few minutes later, the applicants received a second e-mail, which was merely transport-encrypted and in whose text field the password for decrypting the information documents of the previous e-mail could be read in unencrypted form (transport-encrypted e-mail). The password consisted of the combination "first name last name123".

The LDA [redacted] assessed both the sending of the password by unencrypted e-mail (i.e. in plain text) and the password design with a letter to [redacted] dated 24 October 2018 as a data protection violation of Art. 32 GDPR. The reason for this was the corresponding complaint by a [redacted] user of the website [redacted] After becoming aware of the LDA's assessment of the data protection law, [redacted] took the necessary data protection measures with effect from 12 November 2018 to ensure that the process in question complies with data protection law. However, this related exclusively to the handling of requests for information from users of the websites [redacted] This restriction was not communicated to the LDA. [redacted]

The practice of [redacted] of providing information for the [redacted] websites [redacted] until 12 November 2018 is not the subject of the present administrative fine.

In March 2019, the LDA became aware of a complaint from a [redacted] user of the website [redacted] This user complained that he had received the information he had requested in

accordance with Art. 15 (1) GDPR from [redacted] on 8 November 2018 in the manner described above. In the context of the supervisory authority proceedings subsequently initiated by the LDA against the [redacted], the persons authorized to act on behalf of the [redacted] designated the change in the procedure for sending the password for the applicant users of the [redacted] websites [redacted] as a pilot project, which was initially carried out for the [redacted] customer service.

A data protection-compliant adjustment of the technical and organizational measures for sending the password and for password design for the applicant users of the [redacted] websites [redacted] did not take place until 9 July 2019.

The persons authorized to act on behalf of [redacted] knew that, at the latest after the data protection assessment by the LDA had become known, it would have been necessary, at least from 8 November 2018 to 9 July 2019, to redesign the process of sending the password by unencrypted e-mail and the password design "first name last name123" also for the applicant users of the websites [redacted] in such a way that it satisfied the requirements of Article 32 GDPR.

Article 83 (4) (a) GDPR provides:

Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

> (a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; [...]

According to Art. 32 (1) GDPR, the controller and the processor shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

Violated fine regulation: Art. 83 (4) (a) GDPR in conjunction with Art. 32 GDPR

Evidence:

[list of evidence]

We therefore impose the following fine on [redacted] in accordance with Art. 83 (1)–(3) GDPR in conjunction with § 41 Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG). It also bears the costs of the fine proceedings (§§ 464, 465 (1) Code of Criminal Procedure (Strafprozessordnung – StPO) in conjunction with § 46 (1) Law on Administrative Offences (Gesetz über Ordnungswidrigkeiten - OWiG). These consist of the fee (§§ 105 (1), 107 (1) OWiG) and our expenses (§§ 107 (3) No. 2 OWiG).

Fine:	EUR	300.000,00
Fees:	EUR	7.500,00
Expenses:	EUR	3,50
Total:	**EUR**	**307.503,50**

The [redacted] therefore has to pay a total of **EUR 307.503,50.**

Justification of the decision to impose a fine:

[redacted] is the competent authority for conducting administrative offence proceedings for violations of data protection regulations, Art. 51 (1), Art. 58 (2) (i) Art. 83 GDPR in conjunction with § 40 (1) BDSG in conjunction with [redacted]).

Under Article 83 (4) (a) GDPR, infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

> (a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43; [...]

According to Art. 32 (1) GDPR, the controller and the processor shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. Art. 32 (1) (a) GDPR specifically lists the encryption of personal data as a measure.

The [redacted] is the controller to whom the obligations set out in Art. 32 GDPR are directed. Controller under Art. 4 No. 7 GDPR is the natural or legal person, authority, institution or other body which alone or jointly with others decides on the purposes and means of processing personal data. In addition to the [redacted] websites [redacted] and [redacted] also operates the [redacted] websites [redacted]. At least from 8 November 2018 to 9 July 2019, the internal [redacted] Customer Support Team responsible for the [redacted] websites sent an e-mail to which a password-protected document containing the information was attached in response to enquiries from users of these websites who requested information about the data stored at [redacted] in accordance with Art. 15 GDPR. The password for decrypting the in-

formation documents was also sent by e-mail a few minutes later and consisted of the combination "first name last name123". This procedure had been laid down by [redacted], so it decided on the purposes and means of processing personal data.

The procedure for providing information described above was carried out in breach of the provisions of Art. 32 GDPR, in particular Article 32 (1) (a) GDPR. According to this article, the controller and the processor shall take appropriate technical and organizational measures to ensure a level of protection appropriate to the risk, taking into account the state of the art, the implementation costs and the nature, scope, circumstances and purposes of the processing, as well as the varying degrees of probability and seriousness of the risk to the rights and freedoms of natural persons; these measures may include, where appropriate, the pseudonymisation and encryption of personal data. According to Art. 32 (2) GDPR, the assessment of the adequate level of protection to be maintained must take into account in particular the risks associated with the processing, in particular those arising from the destruction, loss, alteration or unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed.

In order to determine which technical and organizational measures within the meaning of Art. 32 (1) and (2) GDPR correspond to the state of the art and are suitable for ensuring a level of protection commensurate with the risk, the recommendations and standards of the Federal Office for Information Security (BSI), in particular the standards BSI-200-1, BSI-200-2 and BSI-200-3[1], can be used. According to these, the first step is to determine the need for protection of the data in question for information purposes in accordance with Art. 15 GDPR. Due to the large number of users of the above-mentioned [redacted], the content of the data in question may vary considerably. They may be subject exclusively to the normal protection requirements, but may also contain extensive data requiring a high level of protection. In accordance with the maximum principle of the BSI IT-Grundschutz,[2] a personal date with a high protection requirement also has an effect on those data which, taken individually, would only fall under a normal protection requirement when assessing the overall protection requirement. Thus, a date with a high protection requirement is sufficient to classify all data concerned as requiring high protection.

In the present case, in the period from 8 November 2018 to 9 July 2019, the [redacted] sent information to the applicants which could include, inter alia, first name, surname, e-mail address, address, telephone number, currency data, a copy of an identity card, Paypal data, the [redacted] This data is highly sensitive in its entirety. The need for protection of personal data depends in particular on the existing risk and its probability of occurrence. Recital 75 GDPR states that risks to the rights and freedoms of natural persons may arise from the processing of personal data which may result in physical, material or non-material harm. The assessment of a possible harm is relevant for the classification of the need for protection of personal data. Recital 75 GDPR states that the processing of personal data may lead to discrimination, identity theft or economic harm.

---

1 BSI, BSI Standard 200-1: Management Systems for Information Security (ISMS), Bonn, 2017.
BSI, BSI Standard 200-2: IT-Grundschutz methodology, Bonn, 2017.
BSI, BSI Standard 200-3: Risk Management, Bonn, 2017.

2 Maximum principle, in: BSI, IT-Grundschutz-Kompendium. Glossary, Bonn, 3rd Edition 2020, p. 41.

The photograph of a person on an identity card is biometric data according to Art. 4 No. 14 GDPR, as this enables the unique identification of a natural person. This is because a photograph contains biometric data if the face of a person is shown on the photograph in the appropriate resolution, orientation and size (cf. Position Paper on Biometric Analysis of the Conference of Independent Data Protection Supervisors of the Federal Government and the Länder (DSK) Version 1.0, as of 3 April 2019, p. 21). Admittedly, processing of this personal data does not constitute processing of special categories of personal data within the meaning of Article 9 GDPR, because biometric data, due to their diversity, are only considered to be such data if they are processed for a special purpose, namely for unique identification and thus in a particularly risky manner (cf. also EDPB guidelines 3/2019 on the processing of personal data by video devices, version 2.0, adopted on 29 January 2020, p. 19, nos. 74, 75). Nevertheless, this personal date is highly sensitive because of its very suitability for identification. The possible considerable damage is due to the fact that, for example, the copy of the ID card can be used for identity theft and, if necessary, for purchases that could result in considerable financial damage for the person concerned. The risk is all the greater if the customers of [redacted] do not independently blacken the copy of the ID card before sending it.

A high level of protection of the personal data contained in the information sent also arises in cases where a copy of the identity card does not need to be sent. This is because even those personal data which result from the [redacted] are suitable for drawing a comprehensive picture of the personality of the person concerned. Depending on [redacted], conclusions can also be drawn about the health or sex life of those affected. This results from [redacted] In addition, it can also lead to widespread damage to reputation or trust if these personal data are disclosed to third parties (cf. BSI 200-2, p. 106f.).

In its statement of 20 March 2020, the [redacted] states that no conclusions can be drawn from the [redacted] sent to it with regard to health or sex life, as it is simply an overview of [redacted]. For this reason, the application of Article 9 GDPR, which deals with special categories of personal data, is also very far-fetched. However, even if these personal data do not fall within the scope of Art. 9 DS-GVO, it is conceivable that the listing of [redacted] may allow conclusions to be drawn, for example, about the sexual orientation of the user. Should such data become known to unauthorized third parties, this could have serious consequences for the persons concerned. In certain cases, it is also possible on the websites operated by [redacted]

That the [redacted], contrary to what it stated in its statement of 20 March 2020, also assumes a high need for protection of the data is clear from the fact alone that it encrypted the information files attached to the e-mail with a password (content encrypted e-mail). This method of encrypting the information files with a password was not criticized by the LDA.

However, [redacted] is wrong in its assumption, expressed in the statement of 20 March 2020, that the technical measures to be taken with regard to the sending of the password are

to be assessed under Article 32 GDPR irrespective of the need for protection of the information to be provided. The [redacted] is of the opinion that the password is not a date particularly worthy of protection, since an unauthorized person would only know the first name and surname and a meaningless sequence of numbers 123. High risks in the event of unauthorized access were therefore not to be expected. For this reason, the standard transport encryption used for e-mails was sufficient for sending the e-mail with the password (transport-encrypted e-mail).

According to the definition of the BSI glossary, a transport encryption [3] is a point-to-point encryption. In the e-mail application, the content is encrypted during transmission between the sender and his e-mail provider, between two e-mail providers among themselves, and between e-mail provider and recipient. The process runs automatically and usually does not require any action on the part of the sender or recipient. At the e-mail provider, the data is decrypted, either for checking (spam, viruses, De-Mail metadata) or, for example, for categorization. This means that only the transport route is encrypted, but the e-mail is unencrypted on the respective e-mail server of the recipient and the sender. In relation to the e-mail with the password, this means that the password was stored on the respective e-mail server in plain text in the e-mail without encryption. But even this type of encryption cannot always be guaranteed, depending on the configuration of the e-mail server (see RFC 7435)[4].

In this respect, transport encryption is not a suitable technical measure within the meaning of Art. 32 GDPR, at least in the case of personal data requiring a high level of protection. The other supervisory authorities, which were listed as examples by [redacted] in its statement of 20 March 2020, represent nothing else in this absoluteness.

In the present case, contrary to the view of [redacted], the password sent by transport-encrypted e-mail is a personal date with high protection requirements. This results from the fact that there is an immanent connection between the first e-mail with the encrypted information files (e-mail with encrypted content) and the second e-mail with the password (e-mail without encrypted content). The second e-mail contains the password for the content of the information files in the first e-mail. Therefore, a high need for protection can also be assumed for the second e-mail, as there is a significant risk of unauthorized disclosure of the personal data contained in the first e-mail with a high need for protection. This is because the compromise of the second e-mail can also compromise the first e-mail. In particular, this risk consists in the fact that the information is sent on the same channel and at close intervals and from the same sender, so that if the e-mail inbox is compromised or the e-mails are tapped, the connection between the two e-mails is very quickly recognized and this can lead to unauthorized disclosure of the information files. There is therefore no room for a separate assessment of the protection needs of the first and second e-mail. This is because it would not be a suitable technical measure if the first e-mail was adequately protected but the key (password) for decrypting the first e-mail could easily be intercepted and read by third parties. As a result, the costly encryption protection for the first e-mail is devalued by the far too low protection of the second e-mail containing the password. To give an example: An expensive bicycle is not connected to the bus stop with an expensive lock and the key is then placed next to it. By the [redacted] would have in the sense of the Art. 32 (1) and (2) GDPR, appropriate technical and or-

---

[3] Transport encryption, in: BSI for Citizens, Glossary, https://www.bsi-fuer-buergerxxx/SharedDocs/Glossareintraege/DE/T/Transportverschluesselung.html , accessed on 18 May 2020

[4] RFC 7435, Opportunistic Security: Some Protection Most of the Time, Internet Engineering Task Force (IETF), 2014. Abrufbar unter https://tools.ietf.org/html/rfc7435.

ganizational measures, commensurate with the risk, should have been taken to protect the password, which at the same time were state of the art. Transport encryption for personal data requiring a high level of protection is not sufficient here.

The objection of [redacted] that the unencrypted presence of passwords protected by transport encryption on the recipient's server cannot be attributed to them because this is after the end of the transmission process and thus in the sphere of the recipient, does not appear to be pertinent. For it is the [redacted] that has chosen the route of transmission and imposed it on the recipient. The recipient of a transport-encrypted e-mail does not even have the possibility to receive this e-mail encrypted on his e-mail server, as this is not provided for by the transport encryption.

A suitable measure for sending the password would have been, for example, multiple authentication, as provided for in measure ORP.4.A21 of the BSI-IT-Grundschutz-Kompendium (Module ORP.4: Identity and Authorization Management) in the case of increased protection requirements.[5]

In addition, end-to-end encryption (e.g. via PGP encryption) would also have come into consideration. With this form of encryption, the content of the e-mail (in contrast to transport encryption) is also encrypted on the respective e-mail server of the sender and the recipient until the authorized person cancels the encryption using a key.

The TeleTrusT - Federal Association for IT Security whose publications are usually used as a benchmark for the "state of the art", also advises to pass on the password to the communication partner in case of password-based PDF or ZIP container encryption, if possible on another communication channel.[6]

In addition to the secure transmission of the password, the password itself must also be state-of-the-art. If password protection is chosen for the encryption of a file, the password used should be correspondingly robust. The complexity of passwords should also prevent possible socializing or guessing of popular password combinations. The complexity of passwords depends, among other things, on the current technical possibilities for cracking such passwords. If instead of the password construct "first name last name123" a password is chosen with the same length, but with no sensible sequence of letters, special characters, further numbers or upper/lower case letters, this results in a significantly higher complexity of the password and thus means a greater possibility of combining possible passwords, so that pure brute force methods for cracking passwords are massively more difficult. A higher password complexity is necessary due to the technologies and methods commonly used today, such as calculations via artificial intelligence or graphics cards. A password of the form "first name last name123" is much easier to crack compared to a password of the form “sdfdfdfg423AsdBB###!” If the knowledge of the password structure chosen by [redacted] had become known, a potential attacker could have decrypted the information file immediately. This would have led to the above mentioned disadvantages for the persons concerned.

For Germany, the Federal Office for Information Security has provided appropriate measures for the creation and transmission of passwords in the module "CON.1 Crypto Concept" and

---

5 BSI, IT-Grundschutz-Kompendium. Glossary, Bonn, 3rd edition 2020.

6 E-mail encryption, p.12, available at https://www.teletrustxxx/fileadmin/docs/publikationen/broschueren/e-mail-verschluesselung/2017-TeleTrusT_E-Mail-Verschl%C3%BCsselung.pdf.

"ORP.4: Identity and Authorization Management" in addition to measure M 2.11 "Regulation of Password Use".[7]

In summary, it is clear that a password based on the "first name last name123" scheme, as generated by [redacted], does not satisfy the state of the art, even if three character classes are used and a minimum length of eight characters is specified.

The persons authorized to act on behalf of [redacted] thus violated Art. 32 (1) (a), (2) GDPR both by sending the e-mail containing the password and by the quality of the password.

The persons entitled to act of the [redacted] committed the violation of Art. 32 GDPR intentionally. Intentional conduct refers to the deliberate realization of the facts of the case in full knowledge of all its circumstances and thus includes both an element of knowledge and an element of will. In a letter dated 24 October 2018, the LDA had already informed the [redacted] of its assessment under data protection law in response to a complaint from a [redacted] user of the [redacted] website [redacted], who complained that the password for decrypting the files had been sent to him in an e-mail (only transport-encrypted) and that the password consisted of "first name last name123". In the letter, the LDA came to the conclusion that the technical and organizational measures taken by [redacted] did not meet the requirements of Art. 32 GDPR. The [redacted] was informed that both the sending of the password in an (only transport-encrypted) e-mail and the quality of the password did not comply with the state of the art and thus constituted a violation of Art. 32 GDPR. [redacted] thereupon adapted the process for [redacted] websites with regard to the sending of the password and, from 12 November 2018, sent passwords by a different means of transmission than the information files (by telephone or by post). The password design was also changed. In a letter dated 16 November 2018, the [redacted] stated that it assumed that "passwords based on the new requirements constitute an appropriate technical and organizational measure to ensure a level of protection commensurate with the risk in accordance with Art. 32 GDPR". This makes it clear that the [redacted] has recognized that the previous measures with regard to password transmission and design were not in conformity with Art. 32 GDPR.

Despite this positive knowledge, the [redacted] did not take over the process of password transmission and design in the same way for the [redacted] websites [redacted]. At least from 8 November 2018, i.e. after receipt of the legal assessment by the LDA, until 9 July 2019, the [redacted] sent the passwords by e-mail and in the variant "first name last name123" through its customer support team responsible for the [redacted] websites. In a letter dated 23 July 2019, [redacted] agreed that the changeover for the [redacted] customer support team would be carried out first and as a pilot project. The changeover for the customer service for the [redacted] had therefore only taken place in a second step. However, waiting for the results of a "pilot project" must not lead to infringements of the GDPR already assessed by the LDA not being taken into account in the process for [redacted] websites in the case of [redacted] websites. [redacted]

[7] BSI, IT-Grundschutz-Kompendium. Glossary, Bonn, 3rd Edition 2020, according to which the character composition of the password must be so complex that it is not easy to guess. A password should consist of uppercase letters, lowercase letters, special characters and numbers. At least two of these character types should be used. If alphanumeric characters can be selected for the password, it should be at least 8 characters long. The number of possible passwords in the given scheme must be large enough to prevent it from being determined in a short time by simple trial and error. In particular, names, license plates, date of birth, etc. must not appear in a password.

[redacted] The assessment of [redacted] expressed in its submission of 20 March 2020 that at no time the requirements of the GDPR had been intentionally disregarded by [redacted] or its employees does not invalidate the accusation of intentional criminal conduct. This is because it is not a precondition for intent within the meaning of the standard that the act was intentional. It is sufficient if the infringement is accepted with approval.

Since the persons authorized to act were aware of the conflicting data protection assessment of the LDA and yet acted in the manner described, they acted intentionally.

The unlawfulness of the act of the persons entitled to act is indicated by the fulfilment of the elements of Art. 83 (4) (a) GDPR in conjunction with Art. 32 GDPR. Reasons to justify the waiver of appropriate technical and organizational measures within the meaning of Art. 32 GDPR could not be considered in the present case.

The acting of its employees is attributable to [redacted]. There is no separation between the violation on the facts side and the substantive liability addressee on the legal consequences side, so that liability is assigned to the entire company. The unlawful act of any person (except for excesses) entitled to act on behalf of the company, regardless of his or her function in the company, is sufficient for the company's liability. Thus, all employees who are entitled to act for the company are covered (*literature reference*). It is not necessary to determine which specific employee acted (*literature reference*).

[redacted] is thus responsible for the administrative offence committed intentionally by its authorized persons.

The need to set and allocate the fine:

Under Art. 58 (2) (i) GDPR, the supervisory authority is authorized to impose a fine under Art. 83 GDPR in addition to or instead of the measures referred to in Art. 58 (2) GDPR, depending on the circumstances of the individual case.

[redacted]

When deciding on the imposition of a fine and on its amount, due account must be taken in each individual case of the criteria set out in Art. 83 (2) GDPR. In addition, Art. 83 (1) GDPR provides that the fine must be effective, proportionate and dissuasive in each individual case. This refers to both the "whether" and the "how" of the imposition of a fine.

In the present case of the sending of the password in a merely transport encrypted e-mail and the password design "first name last name123", it was necessary to impose a fine in particular on account of the following considerations:

A total of 81 persons were affected by the present violation of sending the password in a merely transport encrypted e-mail and using the insecure combination "first name last name123". The period of the breach of the technical and organizational measures under Art. 32 GDPR extended over eight months, i.e. a not insignificant period. The password is a date that requires a high degree of protection, as it is to be seen in combination with the information files that can be decoded by the password. The information files could contain, among

other things, account information of the respective requesting user (e.g. first name, last name, e-mail address, address, telephone number, currency data), a copy of the user's ID, PayPal data, [redacted] Since these sensitive data are particularly worthy of protection, the fact that [redacted] did not take the necessary technical and organizational measures under Art. 32 GDPR to a sufficient extent is of great importance in determining whether a fine should be imposed. Since the password was sent in the same way as the information files (by e-mail), it would have been possible for a third party to access the highly sensitive personal data of the persons concerned. The risk was further increased in particular by the fact that the e-mail containing the password followed the e-mail containing the information files at a very short interval.

The infringement was committed intentionally by the persons entitled to act of [redacted]. The [redacted] had already known since the LDA's letter of 24 October 2018, i.e. before the [redacted] user's complaint, that the LDA did not consider the technical and organizational measures taken by the [redacted] to be sufficient and that the needs of Art. 32 GDPR, were therefore not met. The [redacted] was informed that both the sending of the password in an (only transport-encrypted) e-mail and the quality of the password did not comply with the state of the art and thus constituted a violation of Art. 32 GDPR. Nevertheless, [redacted] operated this procedure in this way for the [redacted] [redacted] web pages. The objection that the conversion of the procedure for the [redacted] web pages was initially a pilot project and that the [redacted] had in no way intentionally infringed the GDPR does not stand up. After all, even waiting for the results of a pilot project does not justify action contrary to data protection. Intention is not decisive for the existence of intent; it is also sufficient to accept it.

Taking into account the way in which the breach was brought to the attention of the supervisory authority, it should be noted that it was only through the complaint of the [redacted] user that the LDA learned that the [redacted] carried out the process of password dispatch and design differently from that of the [redacted] websites. On the basis of the previous advice and assessment with regard to the [redacted] websites and on the basis of the fact that the [redacted] had emphasized in previous proceedings that i[redacted], there was no reason for the LDA to doubt that the process of providing information developed for the [redacted] websites did not also apply to the [redacted] websites. The infringement thus only came to light because a user complained about the procedure.

A fine is an impressive reminder of duties to the person concerned, which is intended to ensure that the person concerned behaves in accordance with the law in future. Violations such as the present one are highly likely to severely damage the confidence of the persons concerned in the lawfulness of the handling of personal data by the bodies concerned. We regularly impose a fine for violations of this kind. For reasons of equal treatment (Art. 3 (1) German Constitutional Law - Grundgesetz (GG)), it was therefore also out of the question to refrain from setting a fine. The decision to impose a fine is proportionate in the present case, since the fine is necessary but also sufficient to remind the [redacted] of their future obligations to comply with data protection requirements.

In the context of the assessment of the fine, particular mitigating factors were the fact that [redacted] cooperated with the LDA in the present administrative offence proceedings. Dur-

ing the hearing, it contributed to clarifying the facts of the case by answering the question posed, thereby helping to determine precisely the number of persons affected by the data protection violation. Another positive aspect is that [redacted] adapted the process of sending and designing passwords for the [redacted] in conformity with data protection regulations promptly after the LDA's letter in the supervisory procedure of 2 July 2019 on 9 July 2019, and has since then operated a user- and data protection-friendly process. The fact that the breach of technical and organizational measures is a formal breach was also taken into account as a mitigating factor. Formal breaches of the GDPR are generally associated with fewer risks for the rights of the persons affected by the data processing. This also took into account the fact that although the [redacted] sent the e-mail with the password insufficiently, since it was only sent in transport-encrypted form, this did not mean that the [redacted] completely waived protective measures under Art. 32 GDPR. In addition, the [redacted] claimed that it had not obtained any financial or other advantages as a result of the infringement of Art. 32 GDPR. This is because the sole purpose of data processing was to grant the data subjects access to their personal data. It is not known that the persons concerned suffered any damage as a result of the process of sending the password. Finally, no other measures pursuant to Art. 58 (2) GDPR were ordered by the LDA with regard to this subject matter in the run-up to the issuance of the administrative fine, which the [redacted] would not have complied with.

On the other hand, it should be noted that the infringement affected 81 users over a period of just over eight months. This formal violation also poses risks for the rights of the persons affected by the data processing, as it cannot be ruled out that the password data may be read by a third party and thus gain access to the encrypted information files. In addition, the authorized persons of [redacted] acted intentionally. Furthermore, the violation only became known to the LDA after the [redacted] gave the impression that [redacted]

The [redacted] has not received an economic advantage by the data protection-violating sending of the password and the password design. Accordingly, this was not to be taken into account.

The upper limit of the fine provided for by law in this respect by wilful misconduct and negligence is EUR 10 million or, in the case of a company, up to 2% of its total annual worldwide turnover in the preceding business year, whichever is the higher.

In the previous financial year (1 January 2019 to 31 December 2019), [redacted] reported worldwide annual sales of approximately [xxx] euros. The upper limit of the fine for the present infringement is therefore approximately [xxx] Euro.

[redacted]

Taking into account the criteria just mentioned, a fine of EUR 300,000.00 is imposed for the deliberate violation of the [redacted], between 8 November 2018 and 9 July 2019, to send the password to the applicant users of the websites [redacted] only by transport-encrypted e-mail and with the design "first name last name123".

The amount of the fine imposed for the present infringement is approximately [xxx] % of the maximum possible amount and is therefore at the lower end of the scale of fines. If one assumes that the maximum amount is set for the most serious cases conceivably committed intentionally and the average value (i.e. [xxx] Euro) for averagely serious cases, it becomes clear that the fine set is far below this value. Measured against the possible range of fines, the fine remains in the lower range.

Nevertheless, the fine imposed fulfils the requirement expressly laid down by the legislator of the GDPR to be effective, proportionate and dissuasive in each individual case. In view of the economic capacity of [redacted], as expressed by its worldwide annual turnover in the preceding business year, and the scale of the present infringement, the fine set at EUR 300,0000.00 is appropriate and does not unduly burden the party concerned. At the same time, the amount of the fine serves to have a deterrent effect and to remind [redacted] emphatically of its obligations to act in accordance with data protection in the future.

Information on legal remedies:
[xxx]

Request for payment:
[xxx]

Data protection legal notice:
[xxx]