WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

Report on the compliance of DMARC with the EU GDPR

eco competence group e-mail

Table of contents

A. Facts

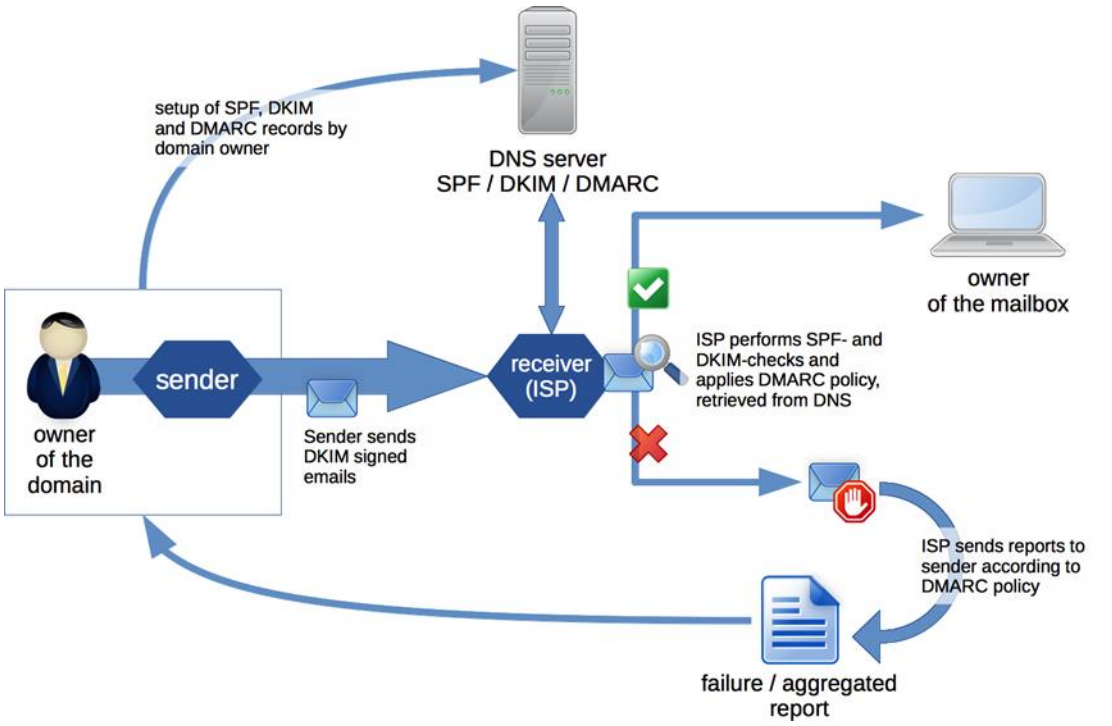
DMARC stands for: Domain-based Message Authentication, Reporting and Conformance: domain-based message authentication, reporting and conformance of messages.[1]

The background to DMARC.org is to increase security in e-mail communication and to ensure greater protection of e-mail recipients against phishing mails, as well as facilitating domain reputation. The goal is to filter out or intercept certain forms of criminal e-mails (phishing) early on so that they do not reach the users.[2] Phishing is the forging of e-mail messages to Internet users, in which, for example, a link contained in the e-mail does not lead back to the reputable provider but rather to the attackers in concealed form, who thus intend to obtain sensitive private data. Phishing can also be done through attachments or requests in an e-mail. Frequently, the sender's address is disguised to simulate a valid sender to the recipient of an e-mail. This is verified, among others, by DMARC in order to detect any "forgeries".

With DMARC as a standard, the aim is to achieve an interaction between the participants in the e-mail communication by an exchange of information taking place between or to them. The following parties need to be differentiated here:

1. The domain owner – e.g. Facebook, Paypal etc. – (or domain administrator who is commissioned by the domain owner to manage all the settings with regard to the domain, including the DMARC entry)
2. The sender who is commissioned by the domain owner to send e-mails, or a third party who sends e-mails under the domain of the domain owner.
3. The Internet Service Provider (hereinafter "receiver") - e.g. GMX, AOL, Hotmail, Yahoo! etc.
4. The report recipient. This can be both the domain owner and the sender or a commissioned legal entity.
5. The recipient to whom the e-mail is to be sent.

[1] https://tools.ietf.org/html/rfc7489
[2] https://tools.ietf.org/html/rfc7489



The sender must first configure SPF (Sender Policy Framework) data records and the public key to DKIM (Domainkeys Identified Mail) for all sending Domains to be taken into account (the DMARC Policy domain). Here, the sender decides which IP addresses and which signatures execute or depict legitimate dispatching of e-mails.

With SPF, the IP address of the sender is compared with a list of IP addresses registered for this domain. With DKIM, e-mails are cryptographically signed on dispatch with a secret code that the receiver can validate by comparing this for "correctness" with the public key. DMARC guarantees the signature integrity based on these two already established technologies.

Using DMARC, the domain owner should now be granted an influence on the handling of non-authenticated messages from the legitimate domains, by defining in DMARC guidelines, in addition to the entries already mentioned above, how the receivers should handle the e-mails in the event of a DMARC authentication test not being passed. A message does not pass DMARC if it does not pass the SPF and/or DKIM test, or only passes in part. For this purpose, a differentiation can be made between a "strict" and "relaxed" approach with regard to the SPF/DKIM authentication.

The starting point here is that DMARC uses the RFC5322 From domain in order to combine/merge authenticated labels.[3]

With a "relaxed" approach with regard to DKIM, the domain "signed" under DKIM and the RFC5322.From domain must be organizationally similar. With a "strict" approach, however, they must tally exactly.

A similar rule applies with a "relaxed" approach with regard to SPF. The RFC53221.MailFrom domain authenticated under SPF and RFC5322.From domain must have the same organizational domain. In the "strict" approach, however, the DNS domain must tally exactly.[4]

In addition, measures such as treating spam (quarantine), rejecting (reject) or no measures (none) can then be defined. (Here, it should be noted that the receiver can also select the rejection or treatment as spam although the e-mail has passed the DMARC authentication test. The receiver can also accept an e-mail that has not passed the DMARC authentication test although the domain owner has defined the rejection in the guidelines.)[5]

In addition to reporting addresses which will be addressed in more detail below, these DMARC Guideline are published as Text Resource Records (TXT RR) in the DNS (Domain Name Service - the directory service for a domain; accessible for anybody).

The reporting address mentioned above serves as a feedback e-mail address to which all (DMARC) participating receivers now send information about these DMARC Policy domains and about the e-mail authentication results.[6] Depending on who was registered for the reports by the domain owner, these individuals now receive information about all incoming e-mails that were presumed to have been sent by this DMARC Policy domain. This information is provided either by means of standardized "aggregated reports" or "failure reports".

It is decisive for the receipt of these reports, who was entered by the domain owner. As explained above, this can be both the domain owner itself or the sender.

[3] https://tools.ietf.org/html/rfc7489
[4] https://tools.ietf.org/html/rfc7489
[5] https://tools.ietf.org/html/rfc7489
[6] https://tools.ietf.org/html/rfc7489

I. Aggregated Reports

Based on the recommendation from DMARC.org, the reports should include the following[7]:

- Sufficient Information for the report recipient, in order to be able to analyze what arrangements were made in accordance with the published guideline as well as SPF, DKIM results.
- Data for each sender subdomain separate From-Mail from the organizational sender domain, also if no guidelines on subdomains were applied.
- Sending and receiving domains.
- The guidelines that were published by the domain owner and the guidelines that were actually applied, if they differ.
- The number of successful authentications.
- The number of messages based on all received messages, even if the delivery was ultimately blocked by other filter systems.

With the aggregated reports, 2 possible types of reports are to be differentiated:

Firstly, there is the option of

- receiving aggregating reports at regular intervals on the corresponding DMARC Policy domains that according to the specifications do not include either individual e-mail addresses or delivery status information (whether it is delivered, whether it is deleted, etc.) and secondly
- aggregated statistics reports on IP addresses that have sent e-mails for the DMARC Policy domain.[8] An IP (Internet Protocol) address is a sequence of numbers for addressing a computer that is assigned to the computer based on the Internet Protocol. Both static and dynamic IP addresses can be considered here during the communication. Whereas a static IP address is firmly assigned to a particular connection owner (to be more exact: the network interface of a certain device of the connection owner); in the case of dynamic addressing an IP address is newly assigned to the connection owner (to be more exact: the network interface of the device of the connection owner communicating with the Internet) with each new take-up of the network connection.[9] The reports contain information about the number of delivered as well as the undelivered e-mails. The first report is sent as soon as a DMARC entry has been published in the DNS.

[7] https://tools.ietf.org/html/rfc7489
[8] http://dmarc.org/presentations/DMARC_general_overview_20120130.pdf p. 13
[9] 1 BvR 1299/05, para. 63; Welp, Information und Recht ("Information and Law"), volume 73, 2009 p.9, 10

The IP report consists of an XML file that includes the following[10]:

- each IP address that has sent e-mails for the DMARC Policy domain
- the number of messages for the DMARC Policy domain from each of these IP addresses
- a statement about how these messages were handled in accordance with the defined DMARC guidelines
- what results authentication by means of SPF and DKIM has revealed.

II. Failure Reports[11]

The failure reports based on message-specific authentication errors can be used to identify any problems in the domain owner infrastructure and to find out the sources and reasons that have caused the sending to fail. They can also be used to assist in tests with regard to the sources and targets of fraudulent messages. These reports refer to individual e-mails that have not passed the DKIM and/or SPF test.

For the sending of failure reports, the AFRF format reveals which data are reported. Here, it involves, among others, the following data:

- The IP address
- The sending e-mail address
- The recipient e-mail address
- The subject of the e-mail
- The e-mail body

It is to be noted that the DMARC authentication refers solely to the DNS domain and not to the local part of an e-mail address labeling/identification found in a message.[12]

[10] http://dmarc.org/faq.html
[11] https://tools.ietf.org/html/rfc7489
[12] https://tools.ietf.org/html/rfc7489

B. Legal appraisal

When checking the compliance of the DMARC procedure with the GDPR from the perspective of companies who want to send DMARC reports, the focus will be placed on the report generation described above and subsequent communication.

Here, aspects of both data protection law and criminal law are to be taken into account.

I. Data protection, in particular the Telecommunications Act

1. Personal data

It is questionable whether as a result of the two reports ("aggregated", "failure"), personal data are processed, whereby due to a lack of independent definitions in the German Telecommunications Act (TKG) the definitions of terms to be found in the General Data Protection Regulation (GDPR, effective since 25 May 2018. Pursuant to Art. 4 Nr. 2 GDPR, processing is "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." Under certain circumstances, in addition to the sender's IP addresses, the data mentioned above may also be collected and processed in the reports, in that these reports are communicated to the respective report recipient.

As the German Telecommunications Act (TKG) does not have its own definition for the term "personal data" either, the general definition in the GDPR is to be used in this regard. Pursuant to Art. 4 Nr. 1 GDPR, personal data are "any information relating to an identified or identifiable natural person." Accordingly, it is decisive that the data refer to a defined or definable private individual, or are suited to establishing a link to a private individual.

When using DMARC, different case constellations first have to be differentiated:

1. The domain owner is a legal entity and at the same time the sender who is entered as the report recipient. It receives the report about the corresponding IP addresses from the receiver.
2. The domain owner is a legal entity and uses one or more legal entities as a sender. The domain owner is registered as the report recipient. It receives the report about the corresponding IP addresses of the senders from the receiver.
3. The domain owner uses one or more legal entities as a sender. One (or more) of the senders is registered as the report recipient. It receives the report with the respective IP addresses from the receiver.
4. A person sends e-mails using the domain of the legitimate owner (phishing)

With regard to the IP addresses that are communicated in the reports, a differentiation needs to be made, as already explained above, between static and dynamic IP addresses. Here, it should be noted that senders, pursuant to best practice, fundamentally do not use any dynamic IP addresses to send e-mails, as primarily spam is sent from e-mail servers with dynamically assigned IP addresses.[13] Nevertheless, it is not to be ruled out that also and particularly in the case of phishing (case 1.4) dynamic IP addresses are communicated by the reports. At any rate, this cannot be clearly determined or negated from the DMARC guidelines.[14]

a) static IP address

The static IP address is unanimously qualified as personal data, as it is potentially possible for anyone to allocate it to its actual owner.[15]

b) dynamic IP address

The previously controversial question as to whether dynamic IP addresses contain personal reference was decided by the highest court of German in 2017 The German Federal Court of Justice (BGH) sees dynamic IP addresses of website visitors as legally protected personal data. The BGH clarified this in a judgment from 16.05.2017[16]. This followed a verdict from the European Court of Justice (EUCJ) from October 2016 on the same topic[17]. According to the verdict, the theoretical possibility of identifying a person on the basis of an Internet address, regardless of whether this is undertaken alone or together with or through one or more third parties (e.g. Internet providers, providers of analytics tools, etc.), is sufficient. The recitals of the GDPR also show that IP addresses are fundamentally personal data. Thus, the recitals for Art. 30 Sentence 1 GDPR: Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags.

[13] http://postmaster.1und1.de/de/fehlermeldungen/; http://postmaster.gmx.de/de/e- mail-policy/
[14] https://tools.ietf.org/html/rfc7489
[15] https://www.datenschutzzentrum.de/ip-adressen/; Härting, Internetrecht (“Internet Law”) 4th edition 2010, para. 91
[16] BGH verdict from 16 May 2017, VI ZR 135/13
[17] EuGH Urteil vom 19 October 2016, C-582/14

c) Domains and other data

Domains are sequences of letters and characters that are assigned to one (or more) IP address(es).[18] Consequently, domains can also have a link to a person, in particular if e.g. they contain the name of a private individual. As it cannot be excluded that e-mail addresses, or other personal data are communicated by means of the failure reports, the reason for the data protection law relevance is to be affirmed.

2. Legislation granting permission/Justification

The processing of personal data is only permitted if it is permitted by law or other legal regulations or the user gives his or her consent to it.

a) Consent

For the cases in which the domain owner is also the sender and/or the sender itself has been registered as the report recipient, consent is to be assumed.

1. Legislation granting permission

a. Sections 91, 88 of the Telecommunications Act (TKG)

With the examples given above (I.1. 1.-3.) the criterion of the private individual is not met as the owner of the static IP address is a legal entity and the link to a private individual cannot be established.[19]

It should, nevertheless, be noted that the Telecommunications Act (TKG) in Section 91 I 2 of the Telecommunications Act (TKG) extends the protected area to legal entities. However, the protection is only extended to the legal entity if data are affected that are subject to telecommunication secrecy pursuant to Section 88 I of the Telecommunication Acts (TKG).[20] Pursuant to Section 88 I of the Telecommunications Act (TKG), telecommunication secrecy covers the "Content of the telecommunication and its associated circumstances, in particular the fact whether someone is or was involved in a telecommunication process". This includes, among others, whether and how often someone set up a telecommunication link, when someone set up a telecommunication link and how long it was set up. Telecommunication secrecy also extends to the associated circumstances of unsuccessful connection attempts.

[18] Fetzer, TKG Kommentar ("Telecommunications ActCommentary"), 2008, Section 3 No.13 para. 67
[19] Comment on Federal Court of Justice (BGH) III ZR 146/10, JurisPR- ITR 15/2011 comment 2, p. 4; Härting, Internetrecht ("Internet Law"), 4th edition 2010, p. 23, para. 94
[20] Fetzer, TKG Kommentar ("Telecommunications Act Commentary"), 2008, Section 91 para. 11

The protective area of Sections 91 et seq. of the Telecommunications Act (TKG) thus also covers connection data of legal entities.[21]

The data of participants and users are protected. Pursuant to Section 3 No. 20 of the Telecommunications Act (TKG), participants are private individuals or legal entities that have a contract for the provision of services with the telecommunications provider. User within the meaning of Section 91 of the Telecommunications Act (TKG) is pursuant to Section 3 No. 14 of the Telecommunications Act (TKG) any private individual who actually uses telecommunication services. As there is no contractual relationship here between domain owner/sender and receiver, nor is the criterion of the user relevant, Section 91 of the Telecommunications Act (TKG) is ultimately not applicable if domain owner and sender are legal entities.

For the sender as a private individual and for the 4th case of phishing mentioned above, however, the link to a person is to be affirmed, in particular with regard to the failure reports as here, as already mentioned, an exclusion of the transmission of personal data is currently not possible.

However, the reach of telecommunication secrecy is questionable.

Pursuant to Section 88 III of the Telecommunications Act (TKG), service providers may not procure knowledge for themselves or others of telecommunication secrets pursuant to Section 88 I of the Telecommunications Act (TKG) beyond the extent required for the commercial provision of the telecommunication services. In addition to the "procurement for themselves", service providers are also prohibited from forwarding telecommunication secrets to third parties.[22] An exception applies here, however, if the Telecommunications Act (TKG) or another statutory regulation makes provision for this.

b. Collection and usage of traffic data, Section 100 Telecommunications Act (TKG) in conjunction with Section 96 Telecommunications Act (TKG)

Permission could result from Section 100 Telecommunications Act (TKG) in conjunction with Section 96 Telecommunications Act (TKG).

Pursuant to Section 100 Telecommunications Act (TKG), the service provider, if necessary, can collect and use user data and traffic data of the participants and users to detect, narrow down or eliminate faults or errors in telecommunication systems.

Pursuant to Section 3 No. 6 Telecommunications Act (TKG), "a service provider is anyone who provides telecommunication services on an entirely or partially commercial basis or collaborates in the provision of such services." This is the case with senders. IP addresses would have to be qualified as traffic data. Pursuant to Section 3 No. 30 of the Telecommunications Act (TKG), traffic data are

[21] Fetzer, TKG Kommentar ("Telecommunications Act Commentary"), 2008, Section 91 para. 11
[22] Ellinghaus, TKG Kommentar (Telecommunications Act Commentary) 2008, Section 88 para. 28

"data that are collected, processed and used in the provision of a telecommunication service." Traffic data refer to a specific telecommunication process.

IP addresses qualify as traffic data in case law[23] Pursuant to Section 96 No. 1 Telecommunications Act (TKG), IP addresses are covered by the term connection data if they are necessary to set up, maintain the telecommunication or for billing.[24] The collection of IP addresses is fundamentally necessary if they are necessary to maintain an Internet connection.

The term fault is to be understood comprehensively as any change unintended by the service provider in the technical equipment used by it for its telecommunication services.[25] The term use can also cover the communication to third parties if this is necessary to eliminate the fault.[26]

It should be noted that, taking into account telecommunication secrecy (Art. 10 I German Federal Constitution [GG], Section 88 of the Telecommunications Act [TKG]) and of the basic right to determination with regard to information (Art. 1 I, Art. 2 I German Federal Constitution [GG]), it is not assumed that in individual cases there are already indications for a fault or an error in the telecommunication systems. Rather, it is sufficient that the data collection and use under question is suitable, necessary and proportionate in the narrower sense in order to combat abstract risks for the functionality of the telecommunication operations.[27]

Although Section 100 of the Telecommunications Act (TKG) intervenes in the aforementioned rights, they can and must be weighed against the justified concerns of the telecommunication companies, public interests and the other interests of the recipients, whereby the principle of proportionality is to be preserved.

Assets are, among others, the telecommunication infrastructure.

This is where the justification of the collection and transmission of the IP addresses could lie as e-mail corresponding is to be kept clear of phishing and spam e-mails and the reports serve to give the domain owners and senders the possibility of gaining further insight into their infrastructure and/or into that of the commissioned sender. Security which is oriented to the interests of the users and the operators is to be guaranteed. If, accordingly, the IP addresses serve to detect and narrow down spam and phishing in order to avoid massive damage and considerable disruption to the telecommunication infrastructure, the collection and transmission is justified. The security, functioning and performance of the telecommunication traffic constitute valuable assets so that the collection and transmission of the IP addresses and other data can take a back seat to them. With regard to the protection of the functioning and performance of the telecommunication infrastructure on the one hand and the protection of sensitive personal data that could cause major

[23] Federal Court of Justice (BGH) III ZR 146/10, para. 23; 1 BvR 256/08, para. 44 et seq.. , Frankfurt Upper Regional Court 13 U 105/07, para. 104; BT- Drucks 15/2316, p. 90
[24] TKG Kommentar ("Telecommunications Act Commentary") 2008, Fetzer, Section 96 para. 6
[25] Federal Court of Justice (BGH) III ZR 146/10 para. 24
[26] TKG Kommentar ("Telecommunications Act Commentary"), 2008, Fetzer, Section 100 para. 3
[27] Federal Court of Justice (BGH) III ZR 146/10 para. 25

damage for the parties affected by phishing on the other, the associated intervention is comparatively small and does not outweigh the legitimate interests, some of which are secured by constitutional law, of the non-legitimate senders and of the recipients and the public interest in the functioning and performance of the telecommunication infrastructure.[28] In particular with regard to the transmission of the IP address, it should be noted that the identity of the respective user cannot be discerned from the IP number and can only be determined through merging with other Information.

c. Consent pursuant to Art. 6 GDPR

If data are transmitted that are not subject to telecommunication secrecy and the Telecommunications Act (TKG) thus does not apply, the collection and use of personal data could be justified under Art. 6 No. 1 Sentence 1 f) GDPR.

Accordingly, the transmission or usage is permissible if it is necessary to preserve justified interests of the responsible organization and insofar as this outweighs the interests or fundamental rights and freedoms of the data subject who requires the protection of their personal data.

In this consideration of interests, a purpose whose pursuit is approved by a healthy sense of justice is decisive, and this is therefore a normative question[29]. The collection and use of the data must not only be expedient to preserve the justified interests, it must also be necessary.

Here, reference can be made to the argumentation already made above.

Conclusion and interim result:

The reports are fundamentally permitted and justified under data protection law. However, the principle of proportionality is to be complied with at all times.

II. Criminal law

Relevant provisions under criminal law are Sections 206 II No. 2 and 303 a I of the Criminal Code (StGB).

1. Section 206 of the Criminal Code (StGB)

If the receiver does not deliver the message, he or she could make himself/herself criminally liable pursuant to Section 206 II No. 2 of the Criminal Code (StGB).

[28] Federal Court of Justice (BGH) III ZR 146/10 para. 31
[29] Gola, DSGVO –Commentary, Art. 6 Rdnr. 51

For this purpose, he or she, as the owner or employee of a company that provides telecommunication services on a commercial basis, would have to suppress a mail entrusted to this company for transmission.

a) Owners within the meaning of Section 206 of the Criminal Code (StGB) are private individuals in their capacity as the responsible persons at the individual commercial enterprises or as (co-) owners of partnerships and corporations if they are also the responsible persons at these companies. Employees are all employees of these companies.

This criterion is met in the case of a provider that offers e-mail services.

b) Pursuant to Section 3 No. 10 of the Telecommunications Act (TKG), commercial provision of telecommunication is the sustainable offering of telecommunication for third parties with or without the intention to generate a profit.

This criterion is also met in the present case.

c) The parcel must be entrusted to the company.

Pursuant to Section 206 II No. 2 of the Criminal Code (StGB), the object of the offence is any form of telecommunication subject to telecommunication secrecy. The e-mail is a suitable object of offence pursuant to Section 206 II No. 2 of the Criminal Code (StGB). The term mail also extends to non-physical items as Section 206 II No. 2 of the Criminal Code (StGB) is not limited, like Section 206 II No. 1 of the Criminal Code (StGB), to sealed mail.[30] A mail is entrusted when it is sent out in compliance with regulations and is in the company's custody. As telecommunication secrecy protects all involved, it must also be assumed that spam and phishing mails are initially covered by the protective area and are covered by the criterion of being sent out in compliance with regulations. In addition, the custody of an e-mail is unproblematic at the latest when the request to send data has reached the mail server of the company and the sending mail server has communicated the data to the receiving server.[31] This is the case here as the e-mails are received by the receiver and it is then determined how these e-mails are to be handled.

d) Suppression requires the mail to be withdrawn from ordinary telecommunication traffic. Suppression is to be assumed when, as the result of technical intervention in the technical process of the sending, transmission or receipt of messages by means of telecommunication systems, the message is prevented from reaching its target, the recipient. [32] e-mail correspondence in particularly is covered by this protective area.[33]

[30] Karlsruhe Upper Regional Court 1 Ws 152/04 para. 21; Fischer, 58th edition, Section 206 of the Criminal Code (StGB), para. 13
[31] Karlsruhe Upper Regional Court 1 Ws 152/04 para. 21
[32] Karlsruhe Upper Regional Court 1 Ws 152/04 para. 22
[33] Fischer, 58th edition, Section 206 para. 15

The criterion is met here by the various options that are defined in the respective guidelines. In particular by the options "reject" and "quarantine" as in this case, the transmission of the incoming e-mail from the receiver to the individual recipient does not take place, or takes place but in modified form. A different evaluation would be given if "quarantine" is implemented through "delivery as spam": In this case, the automatic moving of the mail to a spam folder is evaluated as delivery. In the present case, the recipient still has the option of retrieving the e-mails in the spam folder.

e) The perpetrator would have to act without authorization.

This is not the case if grounds for justification exist. First the explicit or tacit consent that already excludes the satisfaction of elements of an offence and thus the punishability can be considered as grounds for justification for intervention in telecommunication secrecy.

aa) Consent excluding the elements of an offence

It is disputed whether the consent has to be given by all participants in the specific telecommunication correspondence [34] or whether unilateral consent is sufficient. Telecommunication as such is protected, meaning that all participants in this are covered by the protected area.

However, it should be noted here that non-delivery or non-sending of an e-mail is relevant under criminal law, and not the content of the telecommunication as such. The recipient expects the lawful and proper handling of its e-mail. In addition, however, Section 206 of the Criminal Code (StGB) also concerns the interest in the functioning and performance as well as the security of the telecommunication infrastructure. According to the interpretation here, it would thus have to be sufficient if unilateral consent is given by the recipient. Due to the lack of contractual agreements, as a fundamental rule, a presumed consent by the recipient would have to be assumed here with regard to phishing mails in order to avoid further risks to the persons concerned. With regard to the option of the mailbox provider treating certain e-mails as spam, etc., however, this cannot be generally assumed. Rather, it can be concluded from Art. 2 I in conjunction with 1 I of the German Federal Constitution (GG; self-determination with regard to information) that the recipient usually wants to decide himself/herself how he/she wants to deal with such e-mails, i.e. whether he/she wants to read them, ignore them or declare them as spam and move them into the "recycle bin" himself/herself. The assessment whether an e-mail is spam for the respective recipient is subject to individual assessment by the recipient. In practice, the assessment whether an e-mail is spam for the respective recipient is regularly the task of the receiver. This, however, does not affect the right to self-determination with regard to information.

bb) Other grounds for justification

[34] Karlsruhe Upper Regional Court 1 Ws 152/04 para. 23; Fischer, 58th edition, Section 206 para. 9

The criterion "unauthorized" has a twin function.[35] In addition to consent, general grounds for justification can also apply in order to exclude the elements of an offence. However, it should be noted that only sentences of consent can be considered that are set out in a statutory regulation and that explicitly refer to telecommunication processes, Section 88 III 3 Telecommunications Act (TKG).

Here, at any rate, the regulations of the Code of Criminal Procedure (StPO) apply. The transmission of communication content to criminal prosecution authorities can be done based on a valid ruling pursuant to Sections 99, 100, 100 a, 100 b, 100 g , 100 h, 100 i, 101 of the Code of Criminal Procedure (StPO).[36]

Whether in addition general grounds for justification, such as Section 34 of the Criminal Code (StGB), could apply is disputed.[37] In the opinion of Karlsruhe Upper Regional Court that is also followed here, the general grounds for justification also apply if particular case constellations exist that exceed the framework of 88 (3) clause 3 of the Telecommunications Act (TKG).[38] Under certain circumstances, it may therefore be justified to filter out or not to deliver an e-mail as its dissemination could result in faults or damage to the telecommunication and data processing systems, and in addition in the case of phishing further damage cannot be excluded for the parties affected.[39]

Here, the argumentation already presented in detail above can be used again.

[35] Karlsruhe Upper Regional Court 1 Ws 152/04 para. 23
[36] Fischer, 58th edition, Section 206 para. 9
[37] Fischer, 58th edition, Section 206 para. 9
[38] Fischer, 58th edition, Section 206 para. 9
[39] Karlsruhe Upper Regional Court 1 Ws 152/04 para. 25

2. Change in data, Section 303 a of the Criminal Code (StGB)

Punishability could also arise pursuant to Section 303 a (1) Alt. 2 of the Criminal Code (StGB). Section 303 a of the Criminal Code (StGB) protects the interest of the party entitled to dispose of the data.

The statutory offence is relevant if e-mails are suppressed. Reference can be made to the statements on Section 206 (2) No. 2 of the Criminal Code (StGB).[40]

However, a justification can also occur here through presumed consent[41], whereby reference is also made here to the principles presented above in Section 206 (2) No. 2 of the Criminal Code (StGB).

Conclusion: Under criminal law aspects, both Section 206 of the Criminal Code (StGB) and Section 303 a of the Criminal Code (StGB) are met. An exclusion of the punishability, however, can firstly be considered based on an assumed presumed consent by the recipient with regard to the phishing e-mails and secondly based on general grounds for justification, such as the protection of the recipient from fraudulent intentions and the interest of the receiver in maintaining telecommunication security that is an overriding interest.

[40] Fischer, 58th Edition, Section 303 a of the Criminal Code (StGB), para. 10
[41] Fischer, 58th Edition, Section 303 a of the Criminal Code (StGB), para. 13

C. Overall result and recommendations

1. The implementation of DMARC is consistent with the EU GDPR, taking into account restrictions, some of which are considerable.

Whereas the legal implementation of aggregated reports is easier to implement, the expedient implementation of failure reports comes up against considerable doubts under data protection law.

In Detail:

a) With aggregated reports:

The communication of aggregated reports is questionable for data protection law reasons: From a legal perspective, the dispatch IPs included in the reports are to be classified as personal data and are thus subject to the requirements of the Federal Data Protection Act.

For the use of aggregated reports within the framework of the DMARC procedure, this thus means that the report data contained therein may fundamentally be transmitted but the transmission may only be done within the framework of that allowed by law, i.e. to detect and narrow down spam and phishing and to protect the telecommunication systems whilst preserving the principle of proportionality.

An expedient anonymization should be carried out - where possible and reasonable.

b) With failure reports:

Compared to aggregated reports, failure reports contain a large number of personal data that are, however, not absolutely necessary for the effective use of DMARC.

Based on the principle of data economy, it is urgently recommended to resort to redacting in order to avoid personal data of the recipient of a fraudulent mail from being transmitted. These data mandatorily include subject and body of the respective e-mail and the e-mail address of the recipient.

2. Finally, some recommendations need to be given:

a) In order to exclude misuse with regard to the receipt of reports,[42] pursuant to RFC 7489 Chapter 7.1 an authentication and verification system is to be implemented so that it is guaranteed that the specific report recipient is actually authorized and willing to receive the data. With external report addresses, it is recommended, if possible, to have the reports delivered to the DMARC Policy domain and then to forward them to the external report address.

b) In addition, the recipient should be notified about the alternative approach of e-mails and given the authority to decide, in particular with regard to spam mails. At any rate, a procedure with regard to the authority to dispose of the data should be formulated. This can be done in the general terms and conditions of business of the ISP or DMARC guidelines.

[42] https://tools.ietf.org/html/rfc7489#section-7.1