Legal Opinion on the Compatibility of DMARC With the GDPR and Other Legal Provisions

eco E-Mail Competence Group / CSA
Authors: Dr. Katharina Küchler (eco),
Patrick Ben Koetter (sys4 AG)

CSA
Certified Senders Alliance

eco
ASSOCIATION OF THE INTERNET INDUSTRY

Table of Contents

A. Facts of the case

DMARC collects data generated during the delivery of email, processes it to create reports and sends these reports to specific recipients. This expert opinion examines the question of whether and under what conditions the collection, processing, sending and receipt of such reports is legally permissible.

1. DMARC

DMARC is an Internet standard (RFC 7489) and stands for "Domain-based Message Authentication, Reporting and Conformance". Developed to detect and prevent identity misuse in emails, it is used during email transport from a sender to one or more recipients.

Emails that do not pass a DMARC check (DMARC authentication) should be filtered out and not delivered to protect recipients. Owners whose sender domains have been misused to forge identities can also be informed of possible attempts at misuse with DMARC reports. With the data provided by the reporter on the misuse attempt, they can then try to prevent further misuse of their domain.

The DMARC standard provides for two different types of DMARC reports for notifying owners: aggregated and failure reports. These reports differ both in the scope and level of detail of the data they provide, as well as in the frequency with which they are sent.

This report examines whether and under what circumstances one or the other form of the DMARC report is legally permissible against the background of the principle of data minimisation and the protection of personal data.

In order to understand the report, it is necessary to conceptually define the DMARC actors and to further specify the two types of DMARC reports, the aggregated and failure reports, so that it is clear exactly how they differ from each other. The following subsections explain these points in detail.

1.1 Stakeholders

DMARC is used in the exchange of email between a sender and one or more recipients. The actors described below are involved in the exchange and DMARC authentication:

Definition of the actors involved:

Domain holder: In this document, the term 'domain holder' refers to an individual, organisation or delegated individual/organisation that manages the DNS details of a sender domain that publishes a DMARC policy in that sender domain.

Sender: The term 'sender' refers to an individual, an organisation or a service-providing company that sends messages from the domain holder using the sender domain.

Receiver: The term 'receiver' refers to an individual, an organisation or a service provider such as AOL, GMX, Hotmail or Yahoo! that receives the email from a sender domain.

Report recipient: The term 'report recipient' refers to an individual, an organisation or a legal entity commissioned by the domain holder to receive and process DMARC reports for the sender domain in question.

Recipient: The term 'recipient' refers to an individual or an organisation to which the message from a sender domain is addressed and is to be delivered.

1.2 Mode of operation

DMARC requires that a sender domain publishes a DMARC policy that defines who is authorised to send on behalf of the domain and that can be used to identify whether the message was actually sent by that sender domain.

The DMARC policy is published in the form of a DNS record in the DNS zone of the sender domain(s). Focusing on just the essentials for this legal opinion, a DMARC DNS entry specifies:

a) what to do with an email that does not comply with the rules of the email standards SPF and/or DKIM, and
b) whether and how report recipients should be notified of SPF / DKIM rule violations and
c) which form of report – aggregated and/or failure – should be used

In accordance with the DMARC standard and as part of DMARC authentication, the receiving email service (receiver) should then check upon receipt:

1. whether the sender domain used for to transport the email has published a DMARC policy,
2. whether the email submitted for review meets the requirements of SPF and/or DKIM,
3. what to do with the email if it does not stand up to scrutiny and
4. whether the sender domain wishes to be notified of the result of the check in the form of a DMARC report.

The DMARC policy of a sender domain can request an aggregated and/or a failure report and its transmission to one or more recipients. What data is transferred in the reports – this is the relevant aspect for the legal opinion – and why, according to the DMARC standard, differs depending on whether the DMARC report format is aggregated or failure.

1.3 Aggregated reports

Aggregated reports summarise several delivery events in a single report. According to the DMARC standard, a report should include all delivery events from the previous 24 hours and should usually only be transferred once a day.

According to the DMARC standard, an aggregated report should include the following information for report recipients:

- the DMARC policy used
- how the message was handled
- what data was used to verify SPF and what the result of the SPF test was
- what data was used to verify DKIM and the result of the DKIM check
- whether SPF and / or DKIM were in "alignment" with the sender details
- the sending and receiving domains
- the policy specified by the domain owner and the one actually applied by the receiver (if different)
- the number of successful DMARC authentications
- the number of all messages from the sender domain in question, even if they have been blocked or otherwise filtered

1.4 Failure reports

Failure reports provide notification of incorrect DMARC authentication on a case-by-case basis. A failure report should be generated and sent on an ad hoc basis, ideally immediately after an authentication error occurs. It should be more detailed than an aggregated report.

The DMARC specification (RFC 7489) does not specify in Section 7.3. Failure Reports which data items should be transferred. However, it does specify the AFRF format ("Authentication Failure Reporting Using the Abuse Reporting Format", RFC 6591) as the format in which the data should be transferred. A DMARC failure report can be derived from this format and should include, among other things:

- the source IP address of the sender
- the sender's email address
- the recipient's email address
- the subject of the email
- the email body

B. Legal assessment

When assessing the compatibility of the DMARC procedure with existing laws from the perspective of companies wishing to send DMARC reports, the focus is on the report generation and subsequent transmission described above.

Both data protection and criminal law aspects need to be considered.

I. Data protection

1. Personal reference of the transferred data

It is questionable whether personal data is processed by the two types of reports ("aggregated", "failure"). According to Art. 4(1) of the EU's General Data Protection regulation (GDPR), personal data is "any information relating to an identified or identifiable natural person". The decisive factor is, therefore, whether the data relates to an identified or identifiable natural person or is likely to relate to a natural person.

According to Art. 4(2) GDPR, processing includes the "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" of personal data.

1.1 Aggregated reports

As described in section A above, "aggregated reports" contain information about the sending and receiving domains. Domains are sequences of letters and characters that are assigned to one (or more) IP address(es). It is not usually possible to establish a direct personal reference with a domain. A reference to an already identified natural person is, therefore, not initially apparent from the data transferred in an aggregated report. According to the law, however, it is sufficient for a person to be identifiable if they can be identified directly or indirectly, in particular by means of assignment to an identifier. The person, therefore, does not have to be identifiable on the basis of the "date" in question alone, but additional knowledge must always be taken into account.

It is, therefore, questionable whether aggregated reports have an indirect reference to a person through the inclusion of additional knowledge and are therefore considered personal data.

Today, there is no question that domains and IP addresses can be personal data and this has been confirmed several times by the European Court of Justice (ECJ).[1] However, the ECJ's Breyer and Scarlet Extended rulings do not establish that IP addresses can be linked to individuals in general. They instead hold that an IP address alone cannot be personal and that additional information is always required which, in conjunction with the IP address, can then lead to a personal reference. For example, an rdap query (formerly Whois query) could be used to establish a personal reference with regard to domains or IP addresses used.

This raises the question of whose "additional knowledge" is relevant when assessing a personal reference. Is only the knowledge of the data controller relevant in order to make a date personal data or must all additional information known to any third party be taken into account?

For domains below the top-level domain ".de", in particular, the provision of information by DENIC e.G. has been severely restricted since the GDPR came into force. Information about the domain holder can only be requested by third parties in specific cases and by authorised public authorities or holders of affected rights. Third parties without a credible legitimate interest will not receive any information about the domain holder from DENIC.

Therefore, any further data from DENIC e.G. that could lead to the IP address being linked to a person can only be attributed as actually "available" to those data-processing third parties who can credibly prove to DENIC e.G. there has been an infringement of rights by or rights to the domain. If only the knowledge of the data controller were relevant, no personal reference could be made from the basic possibility of a Whois query.

The ECJ rulings in the Breyer and Scarlet Extended cases indicate that the ECJ bases its assessment of personal reference on the perspective of the data controller and not on any additional informa-

1 ECJ case law of 19 October 2016 – C-582/14; ECJ case law of 24 November 2011 – C-70/10.

tion that may be known to anyone.[2] And the ECJ's recent decision on the VIN (vehicle identification number)[3] can also be interpreted as adopting a less broad understanding of personal reference.

The ECJ's Breyer and Scarlet Extended rulings both concerned dynamic IP addresses. However, since the ECJ considered the availability of additional information to be a decisive criterion for the personalisation of dynamic IP addresses, this must also be assumed in the case of static IP addresses. It, therefore, depends on what additional information, and from what sources, is available to the data controller to associate an IP address (and thus a domain) with a natural person.

Static IP addresses, such as those contained in aggregated reports, are, in most cases, only assigned to companies and only in rare exceptional cases to natural persons. Static IP addresses, together with the Whois record, therefore usually have no personal reference. Static IP addresses are, therefore, only rarely personalised, even in combination with Whois records, if the static IP address is exceptionally assigned to an individual natural person for use.

The IP addresses included in DMARC reports are those of the sending Message Transfer Agent (MTA). Although anyone can operate their own MTA, the vast majority of email is sent through MTAs that act as central relays for email from many individual senders. In this case, the IP addresses reported would not be considered personal data as they are not directly linked to a specific individual.[4] This might be different for the IP addresses received, as these are more likely to be natural persons. However, again, the personal link would only be established by the addition of further information attributable to the data controller.

In most cases, therefore, the data transferred in aggregated reports will not be personal data, as it cannot be attributed to a natural person. The scope of the GDPR would, therefore, not apply, and therefore, the transmission of aggregated reports would not require an authorisation basis under data protection law.

1.2. Failure reports

Unlike aggregated reports, "Failure Reports" contain the source and recipient email addresses, subject lines and the body of the email sent. This data is clearly personal data within the meaning of Art. 4(1) GDPR. Therefore, the sending of failure reports can only be justified if one of the authorisation bases of Art. 6(1) GDPR applies.

2 Excursus: The Scarlet Extended ruling concerned the case where the processing of IP addresses was to be carried out by an Internet access provider. Since the provider itself assigns IP addresses to the connections of its customers, it can at any time deduce the identity of its customers from the IP address if this assignment is stored. For this reason, the personal relevance of IP addresses could be affirmed in this case, as the additional information for the assignment of an IP address to a customer identity was directly available here. The Breyer case concerned the processing of IP addresses by a website operator who did not have direct access to the link between IP addresses and customer identities. However, the fact that the ECJ also found that IP addresses could be linked to individuals in this case was primarily due to the wording of the question referred by the German Federal Court of Justice (BGH) and the further assumptions made about the facts of the case. The ECJ understood the question referred by the BGH to mean that the website operator cannot establish the link between the IP address and the identity of the website visitor, but that this link is known only to a third party, namely the Internet access provider. However, the ECJ then explains in paragraphs 47, and 48 that it understands the statements of the BGH on the right of website operators to obtain information from ISPs and on the right of public prosecutors to obtain information from ISPs in the course of investigations (e.g. into cybercrime) to mean that the website operator "obviously has the means that could reasonably be used" to identify the customer or user on the basis of the IP address. On the basis of these considerations, the ECJ only makes a conditional statement on personal data in the judgment. An IP address constitutes "personal data for the provider within the meaning of that provision [...] if it has at its disposal legal means enabling it to identify the person concerned on the basis of the additional information held by the provider of that person's Internet access". The ECJ thus assumes that the possibility of identifying a natural person on the basis of an IP address exists precisely because there is a far-reaching and practically easily enforceable right of access against the Internet access provider. However, this is not the case in Germany.

3 ECJ case law of 09/11/2023 – C-319/22.

4 https://dmarc.org/wiki/FAQ#How_does_DMARC_work.2C_briefly.2C_and_in_non-technical_terms.3F

2. Grounds for justification

The processing of personal data is only permitted if it is authorised by law or other legal provisions or if the data subject has consented. As it cannot be completely excluded that aggregated reports may also contain personal data, the following section examines not only the existence of an authorisation with respect to forensic reports, but also, alternatively, the existence of an authorisation for the sending of aggregated reports.

2.1. Consent

Consent is governed by Art. 7 GDPR. Consent is lawful if it is given voluntarily and unambiguously.

In the case of aggregated reports as well as failure reports, the natural persons behind the sending and receiving domains would have to give their consent to send the report. As the receiving domain is often unaware of the DMARC check, it is very difficult in practice to obtain consent before the report is sent. It would also require the ability to withhold consent or revoke it after the fact. This is also difficult to imagine in practice, or would mean that the person objecting would no longer receive any emails at all. The purpose of the reports is also to combat abuse and phishing. The "unknown" sender or author of a phishing email will, of course, never agree to DMARC reports being sent. The same is true for the recipient of a phishing email. A justification based on consent is therefore excluded.

2.2 Fulfilment of a contractual relationship pursuant to Art. 6(1)(b) GDPR

There is no contractual relationship, at least not with the illegal phishing sender. Nor with the email recipients. A justification for the fulfilment of a contract is therefore also excluded. This applies to aggregated and failure reports

2.3 Legitimate interest pursuant to Art. 6(1)(f) GDPR

The collection and use of personal data may be justified in accordance with Art. (1)(f) GDPR if a legitimate interest exists. A legitimate interest exists if the transfer or use is necessary for the purposes of the legitimate interests pursued by the controller, unless such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data.[5] Where processing is necessary to safeguard a legitimate interest, the interests of both parties must be weighed.[6] All relevant fundamental rights, the intensity of the interference, the nature of the data processed, the nature of the data subject, any tasks or duties, the purposes of the data processing, data security measures, etc. must be taken into account.[7]

2.3.1. Aggregated reports

In the case of aggregated reports, the individual's right to informational self-determination conflicts with the right of companies and the public to exchange data as securely as possible.

When personal data is processed as part of an aggregated report, it will be domain addresses that can be traced back to a natural person. Email content or real names are not sent with aggregated reports and cannot be viewed. The data transferred is therefore very limited.

In contrast, DMARC actively combats phishing, helping to protect individuals and the Internet as a whole. Ultimately, the DMARC process also benefits email recipients, ensuring better protection against cyber-attacks, viruses, bots or harassment from unwanted email. DMARC makes it easier for email providers (e.g. AOL, GMX, Gmail, Yahoo) to ensure that spam and phishing emails never reach the recipient's inbox. In the context of aggregated reports, it can, therefore, be assumed that the legitimate interest of companies, but also of society, in a safer Internet outweighs the interest of individuals in the protection of their informational self-determination. The associated interference with the individual's sphere of protection is comparatively minor with regard to the protection of the functionality and performance of the telecommunications infrastructure and the protection of the personal data of those affected by phishing. The protection of the interests of non-legitimate senders and recipients, some of which are also protected by fundamental rights, must also take second place to these interests. The use of aggregated reports is, therefore,, to be considered proportionate and outweighs conflicting third-party property rights.

5 Schulz, in: Gola, DS-GVO, Art.6, marginal note 52
6 Schulz, in: Gola, DS-GVO, Art.6, marginal note 53
7 Schulz, in: Gola, DS-GVO, Art.6, marginal note 53

2.3.2. Failure reports

In contrast to aggregated reports, failure reports contain considerably more information about both the recipient of the emails and their content. It is, therefore, questionable whether the balance between the individual's right to informational self-determination and the interest of companies and the public in a secure Internet can be struck in favour of the use of failure reports.

For this to be the case, failure reports would first have to be the least intrusive means of achieving the intended purpose, which is to protect against phishing and spam and to protect the Internet.

In principle, this purpose is already served by the aggregated reports, so it could be argued that the 'least intrusive' criterion could already fail. However, the aggregated reports can only show that an attack has taken place. It is not possible to see who initiated the attack. It is, therefore, at least conceivable that aggregated reports may not be sufficient to achieve the objective intended by the failure reports.

Companies would still have to have an overriding interest in achieving the purpose of knowing the actual sender, given the rights of email senders and recipients to anonymity and informational self-determination.

Companies receive a considerable number of emails in the context of failure reports. Even DMARC itself advises that you should only opt in if you are prepared for the flood of data. The argument is that:

> "Failure reports are very useful for forensic analysis to help identify both bugs in your own mail sending software and some kinds of phishing or other impersonation attacks, but... a failure report is sent immediately, every time a receiver rejects a message due to your DMARC policy. The receiver may even send a report if the mail is accepted but one of the authentication mechanism does not pass the alignement (sic) test. A forensic report can be a complete copy of the rejected email in Abuse Reporting Format (ARF). You may think your sending practices are good, and there should be few emails rejected, but every email that spoofs your domain will be rejected too and you are asking to get a copy. This could be several times the volume of your legitimate emails."8

8 https://dmarc.org/wiki/FAQ#How_does_DMARC_work.2C_briefly.2C_and_in_non-technical_terms.3F

The sheer volume of data that a company receives through the regular receipt of failure reports casts doubt on the proportionality of the legitimate interest of the company compared to the interests of the email recipients. Failure reports are sent not only in the case of a phishing or DDOS attack, but in any case where there is any kind of error or deviation from the authentication characteristics of the domain owner. Failure reports may also include reposts for emails where there may simply be an error in the sender address or where an email has been misdirected. However, even in these cases, the recipient of the report will be able to see the email addresses of both the sender and recipient, as well as the content and purpose of their email traffic, even though the discrepancy was not criminal in nature. It is, therefore, not possible to argue that only the email addresses of the criminal sender and the spam content are made public and that this personal data is less worthy of protection because a third-party domain is being illegally misused to carry out phishing and DDoS attacks. The email addresses and content of innocent third parties could also reach the report recipient through the incident reports.

In contrast to aggregated reports, this intrusion cannot be classified as minor, as not only IP addresses are disclosed, but also clearly identifiable email addresses, subject lines and email bodies. The content of communications is an asset that is especially worthy of protection and is therefore protected by Article 10 of the German constitution (Grundgesetz – GG). The sender and recipient of an email have a fundamental right to confidential communication and to ensure that their email addresses are not made available to third parties. The understandable desire of a company to better track errors in its own mailing software must take a back seat to these rights of the individual. The same applies to the legitimate interest in identifying potential risks to one's own infrastructure at an early stage. Only on a case-by-case basis, for example, in the event of a massive phishing or DDoS attack that threatens both the domain owner's infrastructure and the rights of third parties, such as the recipients of such malicious emails, could the receipt of failure reports be justified.

II. Secrecy of telecommunications

Furthermore, the content of emails is data that is protected not only by the GDPR, but also by the right to respect for the privacy of correspondence. This will be explored in the context of German telecommunications law, which specifically governs the secrecy of post and telecommunications ('Fernmeldegeheimnis'). There may be some differences in other jurisdictions

According to Section 3(1) of the German Teleservices Data Protection Act (Telekommunikation-Telemedien-Datenschutz-Gesetz – TTDSG), the "content of telecommunications and its detailed circumstances, in particular, the fact whether someone is or was involved in a telecommunications process", are subject to the secrecy of telecommunications. This means that everything that is sent, transferred or received during the respective telecommunications process is protected.[9] This includes whether and how often someone established a telecommunications connection, when someone established a telecommunications connection and how long it lasted.[10] The "detailed circumstances of telecommunications" also include all "traffic data" within the meaning of Section 3(17) of the German Telecommunications Act (Telekommunikationsgesetz – TKG) and Section 9 TTDSG.[11] The secrecy of telecommunications also extends to the detailed circumstances of unsuccessful connection attempts. The protection of the secrecy of telecommunications is not limited to traditional voice telephony, but is designed to be comprehensive and technology-neutral. In particular, IP-switched communications and email are also covered.[12] The decisive factor is that the communication is not intended for an unlimited group of recipients, but is an individual communication.[13] The information contained in failure reports, such as email addresses, IP addresses, subject line and email body, is, therefore, the content of the telecommunication and its circumstances. The scope of protection of Section 3 TTDSG is open. As the scope of protection of Sections 1 et seq. TTDSG covers connection data of natural persons as well as legal entities, it is also irrelevant here whether personal data is involved or not.[14]

According to Section 3(3) TTDSG, those obliged under the TTDSG may not disclose telecommunications secrets within the meaning of Section 3(1) TTDSG for themselves or others beyond what is necessary for the proper provision of telecommunications services, the operation of a telecommunications network or a telecommunications system. In addition to "obtaining", the obligated parties are therefore also prohibited from disclosing telecommunications secrets to third parties.

Pursuant to Section 3(2) TTDSG, the obligated party is any:

- provider of publicly accessible telecommunications services as well as natural and legal persons involved in the provision of such services,
- provider of telecommunications services offered in whole or in part on a commercial basis, as well as natural and legal persons involved in the provision of such services,
- operator of public telecommunications networks, and
- operator of telecommunications equipment with which telecommunications services are provided on a commercial basis.
- No. 6 TKG: "anyone who provides telecommunications services on a commercial basis, in whole or in part, or assists in the provision of such services."

Senders are, therefore, to be regarded as obligated parties within the meaning of the TTDSG.

By receiving failure reports, the report recipients gain knowledge of email content without this being required for the provision of a telecommunications service. The receipt of failure reports is, therefore, a violation of Section 3(3) TTDSG.

However, according to the TTDSG, access to telecommunications data may be justified if the TTDSG or another statutory provision provides for this.

Section 12 TTDSG could provide a basis for authorisation.

9 Eckhardt, in: TTDSG, Section 3, marginal note 13
10 Eckhardt, in: TTDSG, Section 3, marginal note 15; German Constitutional Court, Decision of the 1st Chamber of the First Senate of 27 October 2006 – 1 BvR 1811/99 –, marginal note 12
11 Eckhardt, in: TTDSG, Section 3, marginal note 14
12 Eckhardt, in: TTDSG, Section 3, marginal note 9
13 Eckhardt, in: TTDSG, Section 3, marginal note 10
14 Eckhardt, in: TTDSG, Section 3, marginal note 11

According to Section 12 TTDSG, the obligated party may, if necessary, process traffic data of end users in order to detect, limit or eliminate disruptions or errors in telecommunications systems. The term "disruption" is to be understood in a broad sense. It refers to any change in the technical equipment used by the obligated party to provide its services that is not intended by the obligated party.[15] For example, it is also a disruption if the IP address ranges used by the Obligated Party are used to distribute malware or spam. This also includes the execution of DDoS attacks. This is because the technology used can no longer perform its intended functions correctly or completely.[16] According to case law, data processing is even permissible to counter abstract threats to the functionality of the technical telecommunications system used. There need not necessarily be evidence of malfunction or error in the individual case.[17] The term "processing" may also include disclosure to third parties if this is necessary for the specific purpose of combating misuse.[18] However, the principle of proportionality must always be respected.[19] The collection and use of the data in question must be appropriate, necessary and, strictly speaking, proportionate to counteract abstract risks to the functioning of telecommunications.

The first question is whether all data contained in failure reports can be classified as traffic data and is thus subject to the authorisation requirement of Section 12 of the German Teleservices Act. According to Section 3(70) TKG, traffic data is "data of which the collection, processing or use is necessary for the provision of a telecommunications service". Traffic data refers to a specific telecommunications process.

Traffic data includes IP addresses, email addresses, date and time of access or delivery, or routing information.[20] Insofar as IP addresses or email addresses are used to detect and limit spam and phishing in order to prevent massive damage and significant disruption to the telecommunications infrastructure, the collection and transmission of such data is justified. The security, functionality and performance of telecommunications traffic provide a high level of protection, so the collection and transmission of IP addresses and other data may be secondary. Failure reports are intended to keep email traffic free of phishing and spam emails, and to allow domain owners and senders to gain further insight into their infrastructure or that of the sender. The aim is to ensure security in the interests of users and operators. Data processing for the purpose of detecting and preventing "disruptions" in the sense of the TTDSG is, therefore, permissible.

However, it is problematic if the entire body of the email or the subject line is visible. This is not traffic data. The justification in Section 12 TTDSG does not apply in these cases.

The transmission of the sender's source IP address, as well as the sender's email address and the recipient's email address, can, therefore, be justified under Section 12 TTDSG. However, the subject line of the email and the body of the email do not qualify as traffic data. If this information is also sent in failure reports, this cannot be justified under Section 12 TTDSG.

15 Eckhardt, in: TTDSG, Section 12, marginal note 27
16 Eckhardt, in: TTDSG, Section 12, marginal note 27
17 Eckhardt, in: TTDSG, Section 12, marginal note 28
18 Eckhardt, in: TTDSG, Section 12, marginal note 73
19 Eckhardt, in: TTDSG, Section 12, marginal note 28

20 Braun, in: Geppert/Schütz, Beck'scher TTDSG-Kommentar, 2023; Rückert, in: MüKo zur StPO 2023, Section 100 a, marginal note 72 et seq.

III. Result of I. and II.

Failure reports are particularly problematic when not only IP addresses but also subject lines and email bodies are sent. This is a serious infringement of the individual's right to informational self-determination. This interference cannot be justified by the fact that phishing or spam can be combated better and more sustainably with the help of the reports than by generating mere aggregated reports. A different result may be reached in individual cases, for example in the case of a particularly massive attack on the network infrastructure of the system concerned. In principle, however, failure reports are not covered by the legitimate interest of the sender. In addition, failure reports that contain subject lines and email bodies are not covered by Section 12 TTDSG and constitute a violation of telecommunications secrecy.

Companies should, therefore, not request failure reports in their DMARC policy, or ensure that failure reports do not contain email bodies or subject lines or redact these so they cannot be read.

Senders of a failure report who have been instructed by the domain holder to send such a report must also check the extent to which they are authorised to send such a report in the first place. They must also check whether they are acting as an independent controller or processor and thus as an "extended arm" of the domain holder. As an independent controller, the sender must also have a basis for authorisation within the meaning of Art. 6(1) GDPR. In this respect, the explanations above apply. It will hardly be possible for the sender to rely on a basis for authorisation. However, even in the case of commissioned processing, this does not mean that the sender can shift the responsibility solely to the domain holder and only act "as instructed". According to Art. 82 GDPR, the principal and the processor are initially jointly and severally liable to the data subjects. Senders should, therefore, avoid supporting failure reports.

Aggregated reports, on the other hand, are compatible with the provisions of both the GDPR and the TTDSG. It is true that the TTDSG also protects the data of legal persons, so that the scope is usually open. However, unlike failure reports, only traffic data is exchanged in aggregated reports. This is protected by the offence of Section 12 TTDSG. However, the principle of proportionality must always be observed. In addition, data should be deleted as soon as it is no longer needed. As a rule, this should be done after seven days, in accordance with the principles of the German Federal Court of Justice on the retention period for Internet service providers.[21]

21 German Federal Court of Justice (BGH) ruling of 03.07.2014, III ZR 391/13.

IV. Criminal law

The relevant criminal provisions in the German Criminal Code (Strafgesetzbuch – StGB) are Section 206(2)(2) on the violation of the secrecy of post or telecommunications, and Section 303a(1) on data manipulation.

1. Violation of the secrecy of post or telecommunications: Section 206 StGB

If the receiver does not deliver a message, they could be liable to prosecution under Section 206(2)(2) StGB.

To do so, as the owner or employee of an enterprise that provides telecommunications services on a commercial basis, they would have to suppress a message entrusted to this enterprise for transmission.

a) Proprietors within the meaning of Section 206 StGB are natural persons in their capacity as owners of the individual commercial enterprises or as (co-)owners of commercial partnerships and corporations, insofar as these also act as company owners. Employees are all employees of these enterprises.

This criterion is fulfilled by a provider that offers email services.

b) Pursuant to Section[22] (10) TKG (old version)1, the sustainable provision of telecommunications for third parties with or without the intention of making a profit is the provision of telecommunications on a commercial basis.

This criterion is also fulfilled in the present case.

c) The transmission must be entrusted to the company

The object of the offence under Section 206(2)(2) StGB is any form of telecommunication subject to telecommunications secrecy. The email is a suitable object of the offence within the meaning of Section 206(2)(2) StGB. The term "transmission" also extends to non-physical objects, as Section 206(2)(2) StGB is not limited to sealed transmissions as is Section 206 206(2)(1)StGB.[23] A transmission is entrusted if it has entered the public domain in the prescribed manner and is in the custody of the company. Since the secrecy of telecommunications protects all parties involved, it must also be assumed that spam and phishing emails are initially covered by the scope of protection and fall under the offence of being put into circulation in accordance with the regulations. It is also unproblematic to assume that an email is in the possession of the receiver at the latest when the request to transfer data has reached the company's mail server and the sending mail server has transferred the data to the receiving server.[24] This is the case here, as the emails are received by the receiver and it is then determined what is to be done with these emails. Suppression presupposes that the transmission is withdrawn from proper telecommunications traffic. Suppression can be assumed if technical intervention in the technical process of sending, transferring or receiving messages by means of telecommunications systems prevents the message from reaching its destination, its recipient.[25] In particular, email traffic is covered by the scope of such protection.[26]

This criterion is met by the various options defined in the relevant policies. In particular, the "reject" and "quarantine" options, as in this case the incoming email is not forwarded by the receiver to the individual recipient or is modified. A different assessment would be made if 'quarantine' was implemented by 'deliver as spam': In this case, the automatic move to a spam folder is considered as delivery. In this case, the recipient still has the ability to access the emails in the spam folder.

e) The offender would have to act without authorisation

This is not the case if there are grounds for justification. The first possible justification for violating the secrecy of telecommunications is express or implied consent, which already excludes the offence and thus criminal liability.

aa) Consent excluding the offence

It is disputed whether consent must be given by all parties involved in the specific telecommunications traffic[27] or whether unilateral consent is sufficient. Telecommunications as such are protected, meaning that all parties involved fall within the scope of protection.

22 The new TKG no longer contains a legal definition of "commercial provision of telecommunications", but the historical and systematic interpretation means that Section 3 (2) No. 2 TTDSG must be interpreted in accordance with Section 3 No. 10 TKG (old version) – see Eckhardt, TTDSG, Section 3 marginal note 73.

23 OLG Karlsruhe 1 Ws 152/04 marginal note 21; Fischer, 58th ed. Section 206 StGB marginal note 13

24 OLG Karlsruhe 1 Ws 152/04 marginal note 21

25 OLG Karlsruhe 1 Ws 152/04 marginal note 22

26 Fischer, 58th ed. Section 206 marginal note 15

27 OLG Karlsruhe 1 Ws 152/04 marginal note 23; Fischer, 58th edition, Section 206 marginal note 9

However, it should be noted that the non-delivery or non-transmission of an email is relevant under criminal law and not the content of the telecommunication as such. The recipient expects the email to be handled lawfully and properly. However, Section 206 StGB also concerns the interest in the functionality, performance and security of the telecommunications infrastructure. In our opinion, it should therefore be sufficient if the recipient has given unilateral consent.

In principle, in the absence of contractual agreements, the recipient's presumed consent should be assumed with regard to phishing emails in order to avoid further risks for the data subjects. However, with regard to the possibility of the mailbox provider treating certain emails as spam or similar, this cannot generally be assumed. Rather, it follows from Art. 2(1) in conjunction with Art. 1(1) of the German Basic Law (informational self-determination) that the recipient usually wants to decide for themselves how they want to deal with such emails, i.e. whether they want to take note of them, disregard them or declare them as spam and put them in the "trash" themselves. The judgement as to whether an email is spam for the respective recipient is subject to an individual assessment by the recipient. In practice, the judgement as to whether an email is spam for the respective recipient is regularly the responsibility of the receiver. However, this does not affect the right to informational self-determination.

bb) Other justifications

The offence of "unauthorised" has a dual function.[28] In addition to consent, general justification grounds can also be used to exclude the offence. However, it should be noted that only authorisations that are stipulated in a statutory provision and that expressly refer to telecommunications processes come into consideration, Section 3(3) TTDSG.

In any case, the provisions of the German Code of Criminal Procedure (Strafprozeßordnung – StPO) come into consideration here. The transmission of communication content to law enforcement agencies can take place on the basis of an effective order pursuant to Sections 99, 100, 100a, 100b, 100g, 100h, 100i, 101 of the StPO.[29]

Whether general grounds for justification, such as Section 34 StGB, can also apply is controversial.[30] According to the Karlsruhe Higher Regional Court, which is also followed here, the general grounds for justification also apply in special cases that go beyond the scope of Section 3(3)(3) TTDSG.[31]Under certain circumstances, it may, therefore, be justified to filter out or not deliver an email because its dissemination causes disruption or damage to telecommunications and data processing systems, in addition, in the case of phishing, further damage to the data subjects cannot be ruled out.[32]

Here again, we can refer back to the argumentation presented in detail above.

2. Data manipulation: Section 303a StGB

Criminal liability could also arise under Section 303a (1) Alt. 2 StGB. Section 303a of the German Criminal Code (StGB) protects the interests of the person authorised to dispose of the goods.

The offence is relevant if emails are suppressed. Please refer to the comments on Section 206(2)(2) StGB.[33]

However, justification can also be provided here by presumed consent[34], whereby reference is also made here to the principles set out above in Section 206(2)(2) StGB.

Conclusion: From a criminal law perspective, both Section 206 StGB and Section 303a StGB are fulfilled. However, criminal liability can be excluded on the one hand due to the presumed consent of the recipient regarding the phishing emails, and on the other hand due to general justification reasons, such as protecting the recipient from fraudulent intentions and the receiver's interest in maintaining telecommunications security, which is an overriding interest.

28 OLG Karlsruhe 1 Ws 152/04 marginal note 23.
29 Fischer, 58th edition, Section 206 marginal note 9
30 Fischer, 58th edition, Section 206 marginal note 9
31 Fischer, 58th edition, Section 206 marginal note 9
32 OLG Karlsruhe 1 Ws 152/04 marginal note 25
33 Fischer, 58th edition, Section 303 a StGB, marginal no. 10
34 Fischer, 58th edition, Section 303 a StGB, marginal no. 13

C. Overall result and recommendations

The implementation of DMARC is compatible with the GDPR, subject to certain limitations.

While aggregated reports can be used lawfully, the implementation of failure reports raises significant data protection concerns.

In detail:

a) Aggregated reports::

In most cases, the IP addresses included in the reports will not be classified as personal data and will therefore fall outside the scope of the GDPR. However, if they do contain personal data, the processing of this data will generally be justified by the company's legitimate interest in error-free email software and protection against spam and phishing, as well as the protection of telecommunications systems. This does not require a specific malfunction.

Appropriate anonymisation should be carried out where possible and reasonable.

b) Failure reports:

Compared to aggregated reports, failure reports contain a large amount of personal data. Therefore, the receipt of failure reports cannot be justified by the legitimate interest of the company, as the interests of the individual in informational self-determination and confidentiality of communication prevail.

The receipt of failure reports can only be justified in individual cases. However, it is recommended that even in such cases, redacting is used to prevent the transfer of personal data of the recipient of a fraudulent email. The information to be redacted must include the subject and body of the email and the recipient's email address.

Legal Opinion on the Compatibility of DMARC With the GDPR and Other Legal Provisions

eco E-Mail Competence Group / CSA
Authors: Dr. Katharina Küchler (eco),
Patrick Ben Koetter (sys4 AG)

eco – Association of the Internet Industry
Lichtstrasse 43h, D-50825 Cologne, Germany
phone +49 (0) 221 / 70 00 48 – 0
fax +49 (0) 221 / 70 00 48 – 111
info@eco.de
international.eco.de

CSA Certified Senders Alliance

eco ASSOCIATION OF THE INTERNET INDUSTRY