Report on the compliance of DMARC with German law

eco competence group e-mail

ドイツ法におけるDMARC準拠に関する報告

eco 電子メールコンピテンスグループ

(訳者: 北崎 恵凡)

WE ARE SHAPING THE INTERNET.

eco

Table of contents

目次

WE ARE SHAPING THE INTERNET.

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 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

A.事実

DMARCとはDomain-based Message Authentication, Reporting and Conformanceの略で、ドメインベースのメッセージ認証、レポーティングおよびメッセージの適合性のことである。

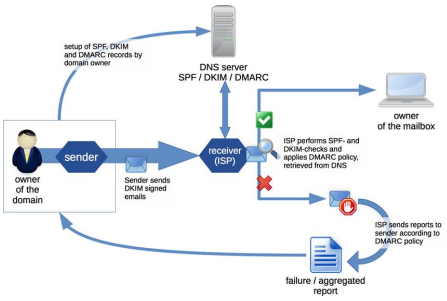
DMARC.orgの背景は電子メールのセキュリティを向上させ、電子メールの受信者をフィッシングメールから確実に保護し、そしてドメインの評価を促進することです。目的は特定の書式の犯罪者の電子メール(フィッシングメール)がユーザへ届く前にフィルタリングまたは傍受することです。フィッシングとはユーザ宛の電子メールを捏造し、電子メールに含まれるURLは信頼できるプロバイダへ誘導されず、むしろ機密の個人情報を取得する目的で隠匿された形式で攻撃者へ誘導される。また、フィッシングは電子メールの添付ファイルや要求を介して行われます。多くの場合、電子メールの送信者アドレスは受信者にとって有効な送信者に偽装されます。これはDMARCにより検証され偽装が検出されます。

標準DMARCは相互に情報交換することにより電子メールの疎通確保を目的としている。当事者は次のように区別される必要があります。

1.ドメイン所有者 - Facebook, Paypalなど (またはドメイン所有者からDMARCレコードを含むドメインに関するすべての設定管理を委託されたドメイン管理者)
2.送信者 - 電子メールを送信するためにドメイン所有者から委託された送信者、または、そのドメイン配下で電子メールを送信する第三者
3.ISP(受信者) - GMX, AOL, Hotmail, Yahoo!など
4.電子メールの受信者

WE ARE SHAPING THE INTERNET.

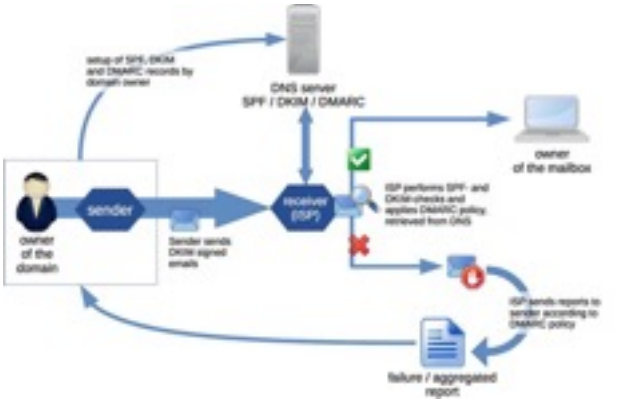
eco



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.



owner of the domain: ドメイン所有者
sender: 送信者
receiver: 受信者
owner of the mailbox: メールボックス所有者

送信者は最初にSPF(Sender Policy Framework)レコードとすべての送信ドメイン(DMARCポリシードメイン)のDKIM(Domainkeys Identified Mail)公開鍵を設定する必要があります。ここで送信者はどのIPアドレスから送信され、どのシグネチャで署名されるかを決定し、送信する電子メールに正当性を示します。

SPFで送信者のIPアドレスは登録されたIPアドレスリストと比較されます。DKIMで電子メールは送信時に秘密鍵で暗号署名され、受信時に公開鍵を使用して正当性を検証できます。DMARCはこれら2つの既に確立された技術に基づいて署名の整合性が保証されます。

DMARCガイドラインを定義することにより、ドメイン所有者はDMARCを使用して正当なドメインからの非認証メッセージの取り扱いに影響を与えることができる。それに加えて受信者がDMARCの検証を通過しなかった電子メールをどのように処理すべきか要求できる。SPFおよび/またはDKIMの検証を通過しなかった、または一部だけを通過した場合、メッセージはDMARCの検証を通過しません。そのため、SPFとDKIMの検証に関して"strict(厳格)"と"relaxed(緩和)"の手段で区別することができる。

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

最初にDMARCは認証ラベルを合わせるためにRFC5322.Fromドメインを用いる。

DKIMに関して"relaxed"の手段ではDKIM署名ドメインとRFC5322.Fromドメインは組織的に類似していなければならず、"strict"の手段では厳密に一致していなければならない。

SPFに関しても"relaxed"の手段では同様の規則が適用される。SPFで認証されたRFC5321.MailFromドメインとRFC5322.Fromドメインは同じ組織ドメイン配下でなければならない。しかし、"strict"の手段ではドメインが厳密に一致していなければならない。

加えて、スパムとして扱う(quarantine(検疫))、拒否する(reject(拒否))、または何もしない(none(なし))という措置を定義することができる。(ここで、受信者はDMARCの検証を通過した場合でもメールを拒否したりスパムとして扱えることに留意すべきである。また、受信者はドメイン所有者がガイドラインに拒否を定義してもDMARCの検証に通過しなかったメールを受信することができる。)

以下に詳細を記載するレポーティングアドレスを含めて、DMARCガイドラインはDNS(Domain Name Service)のテキストリソースレコード(TXT RR)で広報される。

レポーティングアドレスは受信者から送信されるDMARCポリシードメインと認証結果のフィードバック用メールアドレスとして機能する。ドメイン所有者によってレポートのために登録された個々人はDMARCポリシードメインから送信されたと推定されるすべての受信メールに関する情報を受け取る。これらの情報は標準化された"集約レポート"または"失敗レポート"によって通知される。

ドメイン所有者によって登録されたので、これらのレポートの受信で明白です。ドメイン所有者自身または送信者の両方であることができます。

WE ARE SHAPING THE INTERNET.

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

Ⅰ.集約レポート
DMARC.orgからの勧告に基づき、レポートには以下のものを含むべきである。
・SPF、DKIMの検証結果と同様に広報されたガイドラインに基づいて行われた結果をレポート受信者が分析できる十分な情報
・送信者の組織ドメインから分離された送信者の各サブドメインのデータ、またはサブドメインにガイドラインが適用されなかった場合は組織ドメインが適用される
・送信ドメインと受信ドメイン
・ドメイン所有者によって広報されたガイドラインと実際に適用されたガイドライン(もしそれらのガイドラインが異なるのであれば)
・成功した認証の数
・受信したメッセージの総数(最終的に他のフィルタでブロックされた場合でも)
集約レポートの2種類のタイプに区別される。
まず、オプションがあります。
・DMARCポリシードメインに応じた集計レポートを定期的に受信しますが、仕様上、個々のメールアドレスや配信状況に関する情報は含まれません。(それが配信されたか、削除されたか、等)
次に、
・DMARCポリシードメインのメールを送信したIPアドレスに関する集計統計レポート。IP(Internet Protocol)アドレスはアドレス指定のための数字配列であり、インターネット・プロトコルに基づいてコンピュータに割り当てられる。静的および動的IPアドレスともに通信において考慮される。各新しいネットワーク接続において、静的IPアドレスは特定の接続ユーザへ固定で割り当てられる。(より正確には: 接続ユーザの特定のデバイスのネットワーク・インターフェイス); 動的IPアドレスの場合、IPアドレスが新たに接続ユーザへ割り当てられる。(より正確には: 接続ユーザの特定のデバイスのネットワーク・インターフェイス)
レポートにはメールの配信数だけでなく未配信数の情報も含まれる。最初のレポートはDMARCエントリーがDNSで広報されていると送信される。

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

IPレポートには次のものが含まれたXMLファイルで構成される。
・DMARCポリシードメインのメールを送信した各IPアドレス
・これらのIPアドレスそれぞれからDMARCポリシードメインへのメッセージ数
・これらのメッセージがDMARCガイドラインの定義に従って処理されたかについての報告
・SPFとDKIMによる認証結果

Ⅱ.失敗レポート
メッセージ固有の認証エラーに基づく失敗レポートはドメイン所有者のインフラにおける問題点の特定やメール送信失敗の理由と発信源を調べる目的に使用することができる。また、なりすましメッセージの対象と発信源に関して試験を支援するために使用することができる。これらのレポートはDKIMおよび/またはSPFの検証に通過しなかった個々のメールを参照する。
失敗レポートを送信する際はAFRFフォーマットで報告される。
ここで、次のデータが含まれる。
・IPアドレス
・送信者メールアドレス
・受信者メールアドレス
・メールの件名
・メールの本文
DMARC認証はDNSドメインのみ参照するだけでなく、メッセージ中のメールアドレスのローカルパートのラベリングや識別まで参照することに注意すべきである。

WE ARE SHAPING THE INTERNET.

B. Legal appraisal

When checking the compliance of the DMARC procedure from the perspective of German companies who want to send DMARC reports, with the German legal framework, 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 collected, processed or used, whereby due to a lack of independent definitions in the Telecommunications Act (TKG) the definitions of terms to be found in the Federal Data Protection Act (BDSG) apply. Pursuant to Section 3 III of the Federal Data Protection Act (BDSG), collection is the "procurement of data about the person concerned". Pursuant to Section 3 IV of the Federal Data Protection Act (BDSG), processing is "the saving, changing, communicating, locking and deleting of personal data." Pursuant to Section 3 V of the Federal Data Protection Act (BDSG), using is "any use of personal data if it is not processing." Under certain circumstances, in addition to the sender's IP addresses, the data mentioned above may also be collected and processed in the reports by these reports being communicated to the respective report recipient.

As the Telecommunications Act (TKG) does not have its own definition for the term "personal data" either, the general definition in the Federal Data Protection Act (BDSG) is to be used in this regard. Pursuant to Section 3 I of the Federal Data Protection Act (BDSG), personal data are "individual items of information about personal or material circumstances of a defined or definable private individual." 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)

B.法的評価
ドイツ法においてDMARCレポートを送信したいドイツ企業の視点からDMARCの手順遵守をチェックする時、通信上および通信後におけるレポートの生成が焦点となる。
ここでは、データ保護法および刑法の両方の側面で考慮されるべきである。

Ⅰ.データ保護、特に電気通信法

1.個人データ
電気通信法(TKG)には独立した定義が不足しているため、2つのレポート(“集約”、”失敗”)の結果として個人データが収集、処理、使用されるかどうか疑問の余地があり、連邦データ保護法(BDSG)の用語の定義が適用される。連邦データ保護法(BDSG)の第3項第3文に基づき、収集は「当事者に関するデータの入手」である。連邦データ保護法(BDSG)の第3項第4文に基づき、処理は「個人データの保存、変更、通信、保護、削除」である。連邦データ保護法(BDSG)の第3項第5文に基づき、使用は「個人データが処理されていない時の使用」である。特定の条件下において送信者のIPアドレスに加えて上記のデータは収集され、それぞれのレポート受信者へ伝達されるレポートの中で処理される。

電気通信法(TKG)には”個人データ”の用語の定義がありません。そのため連邦データ保護法(BDSG)の一般的な定義が使用されることになる。連邦データ保護法(BDSG)の第3項第1文に基づき、個人データは「特定または特定可能な個人の固有情報または物質の詳細情報」である。したがって、特定または特定可能な個人情報を参照するデータ、または個人に紐づけるのに適したデータである。

DMARCを使用する際は、異なるケース集合も最初に区別する必要がある。
1.ドメイン所有者は法人であると同時にレポートを受信する送信者である。受信者からIPアドレスに関するレポートを受信する。
2.ドメイン所有者は法人であると同時に送信者として1つ以上の法人組織を使用する。ドメイン所有者はレポート受信者として登録される。受信者から送信者に相当するIPアドレスに関するレポートを受信する。
3.ドメイン所有者は送信者として1つ以上の法人組織を使用する。1つ(またはそれ以上)の送信者はレポートの受信者として登録される。受信者からそれぞれのIPアドレスを含むレポートを受信する。
4.個人が正当な所有者(フィッシング)のドメインを使用してメールを送信する。

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 possible for anyone to allocate it to its actual owner.[15]

b) dynamic IP address

Whether dynamic IP addresses can be qualified as personal data, however, is disputed as there is no allocation as in the case of a static IP address. The starting point for the difference in opinion is the criterion of "determinability" pursuant to Section 3 I of the German Data Protection Act (BDSG). The allocation to a dynamic IP address is merely done temporarily by the Internet access provider. An anonymity of the Internet users is guaranteed here. Even if the IP address can be read by server operators, a longer-term connection of the IP address with a name by which the user would become known is not possible.[16] From the IP address as such there is no direct link to a certain person, meaning that this would first have to be established.[17]

As only the access provider assigns the IP address and therefore the link to a person is possible for it without considerable effort, the cases described above are disputed in which other persons such as here the mailbox provider, collect and communicate dynamic IP addresses.

[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] Nietsch, CR 11/2011, p. 764
[17] Comment on Federal Court of Justice (BGH) III ZR 146/10, jurisPR- ITR 15/2011 p.4

レポートで通信されるIPアドレスに関しては既に上述したように静的および動的なIPアドレスとで区別される必要がある。ここで、ベストプラクティスに基づき、主に迷惑メールが動的IPアドレスを用いてメールサーバから送信されるように、電子メールを送信するために基本的に任意の動的IPアドレスは使用されないことに注意するべきである。それでも、動的IPアドレスはレポートで通知され、特にフィッシングの場合(ケース1.4)においては除外されるべきではない。いずれにせよ、DMARCガイドラインからは明らかに決定または否定できない。

a) 静的IPアドレス
静的IPアドレスは誰にも実際の所有者に割り当てることが可能であるため、個人データに該当する。

b) 動的IPアドレス
動的IPアドレスは静的IPアドレスのように割り当てられないため、個人データに該当するかどうか争われている。意見の相違の出発点はドイツデータ保護法(BDSG)の第3項第1文の「特定可能性」の基準である。動的IPアドレスはISPによって一時的に単に割り当てられるものである。インターネットユーザの匿名性はここで保証されている。IPアドレスがサーバ運用者によって読み取ることができたとしても、IPアドレスの長期接続によりユーザ名を知られることは不可能である。特定の人への直接リンクが無いIPアドレスから最初に確立されなければならない。

ISPのみがIPアドレスを割り当てるため、それ相当の努力もせず人へのリンクが可能であり、上記の例では、メールボックスプロバイダのような他の人が動的IPアドレスを収集、通信することが争点である。

WE ARE SHAPING THE INTERNET.

aa) Relativity of the link to a person

One interpretation[18] assumes the relativity of the link to a person and bases the evaluation of the determinability pursuant to Section 3 I of the Data Protection Act (BDSG) on whether the organization responsible can establish the link to a private individual with the means normally at its disposal and without disproportionate effort. In particular, a differentiation is made based on whether the de-anonymization is possible with proportionate effort. This, however, is only possible for the access provider.[19] A third party (here the mailbox provider) could determine the user behind the IP address only with the help of the access provider who, however, due to a lack of legal basis, may not make this information available to third parties. The theoretical possibility of identifying the user cannot correspond to the aforementioned definition of determinability.[20]

bb) Objectivity of the link to a person

According to this interpretation, it is not relevant whether disproportionate effort is required in order to de-anonymize the IP address. It is only sufficient that the theoretical option of linking the IP address to a private individual exists in some form.[21] It is not relevant whether a determinability of the individual in the legal sense is only given if the person can be identified by legal means. Data protection law should precisely protect against the misuse of data so that such a restriction in the term of determinability does not appear justified.[22] The objectivity of the link to a particular person is also based on Recital 26 of the data protection directive 95/46/EC.[23] The Art. 29 Group also assumes the absolute term. In Recital No. 26 of the EU Data Protection Directive 95/46/EC, it is clearly determined that all means are to be taken into account that can be used by the party responsible for the processing or by any other person after reasonable assessment for the identification of the respective person to ascertain whether a person can be determined.[24]

As it cannot be excluded that third parties have the necessary additional knowledge to establish a link to a person, only the probability of a possible identification to be assessed de facto is relevant for the link to a particular person.[25] With dynamic IP addresses too, these can be assigned to individual connections and thus, if applicable, to private individuals by third parties with the help of the log files of the Internet Service Provider (ISP). Therefore, at least referenceability of the

[18] Eckhardt, CR 2011/5 (p. 342 with further references); Härting, Internetrecht ("Internet Law"), 4th edition 2010, p. 23 para. 94
[19] Munich Regional Court 7 O 1310/11, para. 120
[20] Munich District Court 133 C 5677/08, para. 22-24; Eckhardt CR 5/2011 p. 342
[21] Härting, Internetrecht ("Internet Law") 4th edition para. 93
[22] Berlin Mitte District Court 5 C 314/06 para. 13, 14
[23] WP 136 (01248/07/DE of Article 29 Data Protection Group, p. 21 et seq.; WP 148 (00737/DE) of Article 29 Data Protection Group, p.9; Stiemerling/Hartung CR 1/ 2012, p. 64
[24] WP 136 (01248/07/DE of the Article 29 Data Protection Group p.17 et seq.
[25] Welp, Information und Recht ("Information and Law"), volume 73, 2009 p. 206

aa)人へのリンクの相対性
一つの解釈は人へのリンクの相対性を想定し、データ保護法(BDSG)の第3項第1文に基づき、その処分と不均衡な努力無しに通常の手段で個人へのリンクを確立できる責任のある組織かどうかについて特定可能性の評価を基礎とする。具体的には比例努力で非匿名化が可能かどうかに基づいて区別されます。しかしながら、これは唯一ISPが可能です。第三者(ここではメールボックスプロバイダ)がISPの助けを借りてIPアドレスの背後にあるユーザを特定することができるが、法的根拠の不足のため、第三者がこの情報を利用できるようにはしないだろう。ユーザを特定する論理的可能性では前記の特定可能性の定義に相当しない。

bb)人へのリンクの客観性
この解釈によれば、IPアドレスの非匿名化のために不均衡な努力が必要であるかどうかは関係しない。IPアドレスを個人へリンクする理論上のオプションがいくつかの形式で存在するだけで十分である。合法的手段で人を特定できる場合のみ、法的な意味での個人の特定可能性が与えられるかどうかは関係しない。データ保護法は正確にはデータの不正使用から保護される必要があるので、特定可能性の制限では正当化されない。特定の人へのリンクの客観性はまた、データ保護指令(95/46/EC)の前文26に基づいている。第29条では絶対的な用語を定義している。EUデータ保護指令(95/46/EC)の前文26に、処理の責任当事者、または人物を特定できるかどうかを確かめるためにそれぞれの人物の特定に関する合理的な評価を受けた他の者によって使用されるすべての手段が考慮されるべきであると明らかに定義されている。
第三者が個人へのリンクを確立するために必要な追加の知識を持っていることを排除できないようになっている。事実上評価されている唯一の特定可能性は特定の個人へのリンクに関連している。個々の接続に割り当てられる動的IPアドレスも、ISPのログファイルの助けを借りて第三者によって個人へ割り当てることが可能である。そのため、少なくとも

dynamic IP address to a particular person and thus of the application of data protection laws must be assumed.[26]

cc) Interim result:

According to the opinion here, the better reasons are in favor of the objectivity of the link to a particular person; at any rate, it is to be assumed in cases of doubt for the higher-level purpose, namely the protection against phishing and spam, that dynamic IP addresses constitute personal data. As it cannot be excluded that third parties have the necessary additional knowledge to establish a link to a person, the possibility of a potential link actually to be assessed is therefore relevant for the link to a particular person.

c) Domains and other data

Domains are sequences of letters and characters that are assigned to one (or more) IP address(es).[27] 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 collection, processing and usage 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.[28]

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

[26] https://www.datenschutzzentrum.de/ip-adressen/
[27] Fetzer, TKG Kommentar ("Telecommunications ActCommentary"), 2008, Section 3 No.13 para. 67
[28] 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

動的IPアドレスの特定の個人への参照可能性とデータ保護法の適用は想定される。

cc)暫定結果
ここでの意見では、より良い理由として特定の人へのリンクの客観性を支持する。より高いレベルの目的の疑いの場合に想定される、すなわちフィッシングやスパムに対する保護で、動的IPアドレスは個人データを構成する。第三者が個人へのリンクを確立するのに必要な追加の知識を持つことを排除できないように、実際に評価される可能性のあるリンクは特定の人へのリンクに関連する。

c) ドメインおよびその他のデータ
ドメインは１つ(またはそれ以上)のIPアドレスに割り当てられた文字と文字の配列である。そのため、ドメインはまた、特定の人へのリンクを持つことができる。すなわち、個人の名前を含む場合である。失敗レポートにより通知されるメールアドレスまたは個人データを除外することはできないため、データ保護法の関連性が肯定されるべきである。

2.許可/正当性を付与する法律
法律や他の法規制によって許可されている場合、またはユーザが同意している場合のみ、個人データを収集、処理および使用が許可される。

a)同意
ドメイン所有者が送信者、および/または送信者自身がレポートの受信者として登録されている場合に同意が想定される。

1.許可を与える立法

a.電気通信法(TKG)の第91項, 第88項

上記(Ⅰ.1.1.-3.)の例では、固定IPアドレス所有者が法人だと個人へのリンクが確立されないように、個人の基準は満たしていない。
だが、電気通信法(TKG)の第2章第91項において電気通信法(TKG)が保護された領域を法人へ拡張していることに留意すべきである。しかし、

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).[29] 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.

The protective area of Sections 91 et seq. of the Telecommunications Act (TKG) thus also covers connection data of legal entities.[30]

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.[31] 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).

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

電気通信法(TKG)第1章第88項 通信の秘密に基づき、データが影響を受ける場合にのみ保護が法人へ拡張される。電気通信法(TKG)第1章第88項に基づき、通信の秘密は"特に誰かが通信に関与しているかどうかという事実において通信の内容とそれに関連する状況"を対象とする。これは、誰かがどのくらいの頻度で通信リンクを確立させたかどうか、いつ通信リンクを確立させたか、どのくらいの長さ(時間)通信リンクが確立されたか、ということも含む。また、通信の秘密は失敗した接続試行の関連状況にも及ぶ。

こうして電気通信法(TKG)第91項の保護領域は法人の接続データにも及ぶ。

参加者やユーザのデータが保護されています。電気通信法(TKG)の第3項第20号に基づき、参加者は通信プロバイダとのサービス契約をしている個人または法人である。電気通信法(TKG)の第91項におけるユーザとは第3項第14号に準ずる実際に通信サービスを使用するすべての個人である。ドメイン所有者/送信者と受信者との間に契約関係はないので、ドメイン所有者と送信者が法人である場合には、電気通信法(TKG)の第91項の基準で関連するユーザではなく、最終的には適用されない。

しかし、個人としての送信者のため、また前述したフィッシングの第4のケースのため、特に失敗レポートに関して個人へのリンクは肯定されるべきである。既に述べたとおり、個人データの送出の除外は現在不可である。

しかし、通信の秘密の範囲が疑問である。

電気通信法(TKG)の第88項IIIに基づき、サービスプロバイダは通信サービスの商用提供に必要な範囲を超えて、電気通信法(TKG)の第88項Ⅰに基づく自分自身、または他人の通信の秘密を知り得ない。自分自身のことを知ることに加えて、サービスプロバイダは第三者へ通信の秘密を転送することが禁じられている。しかし、これに対して電気通信法(TKG)または別の法規制が規定される場合は例外が適用される。

b.電気通信法(TKG)の第96項と共に、電気通信法(TKG)の第100項のトラフィックデータの収集と利用

電気通信法(TKG)の第96項と共に、電気通信法(TKG)の第100項から許可される場合もある。

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 "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[32] 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.[33] 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.[34] The term use can also cover the communication to third parties if this is necessary to eliminate the fault.[35]

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.[36]

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

[32] 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
[33] TKG Kommentar ("Telecommunications Act Commentary") 2008, Fetzer, Section 96 para. 6
[34] Federal Court of Justice (BGH) III ZR 146/10 para. 24
[35] TKG Kommentar ("Telecommunications Act Commentary"), 2008, Fetzer, Section 100 para. 3
[36] Federal Court of Justice (BGH) III ZR 146/10 para. 25

電気通信法(TKG)の第100項に基づき、サービスプロバイダは必要に応じて、通信システムの故障やエラーを検知、絞り込み、除去するためにユーザデータと参加者およびユーザのトラフィックデータを収集し使用することができる。

電気通信法(TKG)の第3項第6号に基づき、サービスプロバイダとは通信サービスを商業ベースまたは協業により完全にまたは部分的に提供する者である。送信者の場合、IPアドレスはトラフィックデータとみなされる。電気通信法(TKG)の第3項第30号に基づき、トラフィックデータとは通信サービスの提供で収集、処理、使用されるデータである。トラフィックデータは特定の通信処理を参照する。

IPアドレスは法律ではトラフィックデータとみなされる。電気通信法(TKG)の第96項第1号に基づき、電気通信の開始や維持、または課金のために必要であれば、IPアドレスは接続データとして扱われる。IPアドレスの収集はインターネット接続の維持に必要であれば基本的に必要である。

障害とはサービスプロバイダの通信サービスのための装置における意図しない変化として包括的に理解されるべきである。使用とは障害を除去するために必要であれば第三者への通信もカバーすることができる。

通信の秘密(ドイツ国憲法[GG]第10条、電気通信法[TKG]第88項)と情報に関する基本的権利(ドイツ国憲法[GG]第1条、第2条)は留意すべきだが、個々のケースで通信システムの故障やエラー兆候が既にあることは想定されていない。むしろ、通信動作の機能に対する抽象リスクとの戦いのために、疑問がある中でのデータの収集、使用は適切であり、必要であり、狭い意味で釣り合っている。

前述の権利に電気通信法(TKG)の第100項が干渉するが、通信会社の正当化された懸念、公共の利益、受信者の他の利益に対して比較検討されなければならない。それにより比例の原則は維持される。

資産は、とりわけ、通信インフラである。

電子メールをフィッシングや迷惑メールから隔離するためにIPアドレスの収集と送信の正当化があり、レポートはドメイン所有者と送信者へそれらのインフラ、および/または委託された送信者のインフラに関して更なる理解を促す可能性を与える。

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 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-legitmate senders and of the recipients and the public interest in the functioning and performance of the telecommunication infrastructure.[37] 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 Section 28 of the Federal Data Protection Act (BDSG)

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 Section 28 I 1 No. 2 or II of the Federal Data Protection Act (BDSG).

Accordingly, the transmission or usage is permissible if it is necessary to preserve justified interests of the responsible organization and there is no reason to assume that this is outweighed by the protectable right of the party concerned to the exclusion of the processing or usage.

In this consideration of interests, a purpose whose pursuit is approved by a healthy sense of the law is decisive. The collection and use of the data must not only be expedient to preserve the justified interests, it must also be necessary.[38]

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.

[37] Federal Court of Justice (BGH) III ZR 146/10 para. 31
[38] Gola, Klug, Körffer, BDSG Kommentar (Federal Data Protection Act Commentary), 10th edition 2010, Section 28 para. 25

ユーザとオペレータの利益の中心となるセキュリティは保証されるべきである。従って、IPアドレスは通信インフラへの大規模な被害と大きな混乱を避けるために、迷惑メールとフィッシングの検知と絞り込みに役に立ち、収集と送信は正当化される。セキュリティに関して、IPアドレスやその他のデータの収集および送信がセキュリティのために目立たない立場となるように、通信トラフィックの機能と性能は貴重な資産を構成する。通信インフラの機能と性能の維持がある一方で、フィッシングにより深刻な影響を引き起こす可能性のある機密性の高い個人データの保護もあることに関して、関連する干渉は比較的小さく、正当な利益を上回らず、通信インフラの機能と性能における不当な送信者の利益、受信者の利益、公益は憲法により守られる。特にIPアドレスの送信に関しては、それぞれのユーザの身元はIP番号からは識別することができず、その他の情報と組み合わせることで特定することができることに留意すべきである。

c.連邦データ保護法(BDSG)の第28項に基づく同意

通信の秘密の対象とならないデータが送信された場合、電気通信法(TKG)の対象とはならず、個人データの収集および使用は連邦データ保護法(BDSG)の第28項第1文第2号または第2文のもとで正当化される。

したがって、責任のある組織の正当化された利益を守る必要がある場合には送信または使用は許可される。処理または使用の排除に関係する当事者の保護された権利を上回ることを前提とする理由はない。

利益の考察では、その目的の実行が法律の健全な感覚によって認められることは決定的である。データの収集および使用は、正当化された利益を守るために好都合なだけではいけず、必要でなければならない。

ここで、上述の議論を参照できるようになった。

まとめと中間結果:

レポートは基本的にデータ保護法のもとで許可され、正当化される。しかし、比例の原則は常に遵守されるべきである。

WE ARE SHAPING THE INTERNET.

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).

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.[39] 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

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

Ⅱ.刑法

刑法の関連規定は刑法(StGB)の第206項第2文第2号および第303a第1文である。

1.刑法(StGB) 第206項

刑法(StGB)の第206項第2文第2号に基づき、受信者がメッセージを配信していない場合、彼または彼女は彼自身/彼女自身に刑事責任を負わせることができる。

この目的で彼または彼女は商業ベースの通信サービスを提供する会社の所有者または従業員は配送会社へメールを委託するのを規制しなければならない。

a) 刑法(StGB)の第206項における所有者とは個々の商業企業の責任者として、または共同経営会社や企業の責任者である(共同)所有者の能力を持つ個人である。従業員はこれらの企業すべての従業員である。

この基準は電子メールサービスを提供するプロバイダも適用される。

b) 電気通信法(TKG)の第3項第10号に基づき、通信の商業規定は利益を生むことを意図する、意図しないに関わらず第三者のための持続可能な通信商品である。

この基準は本ケースに適用される。

c) 郵便小包は会社へ委託する必要がある。
刑法(StGB)の第206項第2文第2号に基づき、犯罪の目的は通信の秘密に該当する任意の通信形式である。刑法(StGB)の第206項第2文第2号に基づき、電子メールは犯罪に適当な目的である。メールの用語は刑法(StGB)の第206項第2文第2号として非物理的なアイテムにも拡大され、刑法(StGB)の第206項第2文第1号のように密封されたメールに限定されない。規制に準拠してメールを送る時にメールは委託され、会社の管理下にある。通信の秘密は関係するすべてを保護し、また迷惑メールやフィッシングメールは最初は保護領域の対象となり、規制に準拠して送信される基準の対象になると仮定されなければならない。加えて、データ送信要求が会社のメールサーバへ届いて、送信メールサーバから受信サーバへデータを送信する際、電子メールの監督権はいくら遅くとも問題ない。

communicated the data to the receiving server.[40] 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. [41] e-mail correspondence in particularly is covered by this protective area.[42]

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 [43] 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

[40] Karlsruhe Upper Regional Court 1 Ws 152/04 para. 21
[41] Karlsruhe Upper Regional Court 1 Ws 152/04 para. 22
[42] Fischer, 58th edition, Section 206 para. 15
[43] Karlsruhe Upper Regional Court 1 Ws 152/04 para. 23; Fischer, 58th edition, Section 206 para. 9

これは電子メールが受信者によって受信され、電子メールが処理される方法が決定されるケースである。

d) 抑止は通常の通信トラフィックからメールを取り出す必要がある。抑止は通信システムによる技術的なメッセージの送信、転送、受信の処理における技術的な介入の結果、メッセージが目標の受信者へ届くのを妨げられる時に想定される。電子メールの通信は特にこの保護領域でカバーされる。

基準はそれぞれのガイドラインで定義される様々なオプションによって満たされる。特に"拒否"と"検疫"のオプションにより、受信機から個々の受信者へ流入してくる電子メールの送信は行われない、または変更された形式で行われる。"検疫"が"迷惑メールとして配送"の実装では別の評価がされる。この場合、メールの迷惑メールフォルダへの自動移動は配送として評価される。この場合、受信者はまだ電子メールを迷惑メールとして取得するオプションがあります。

e) 加害者は許可なしに行動しなければならない
正当化の根拠が存在する場合、これは当てはまらない。最初に明示的または暗黙の同意が既にあれば犯罪の要素を満たさず、通信の秘密の侵害の正当化の根拠として罰則の可能性が考えられる。

aa) 犯罪の要素を取り除く同意
特定の通信において同意がすべての参加者へ提供されるべきかどうか、または一方向の同意で十分かどうかが係争される。通信はすべての参加者が保護領域でカバーされるという意味で保護される。

しかし、電子メールの不達、または未送信は通信の内容ではなく、刑法に関連することに留意すべきである。受信者は電子メールの適法且つ適切な取り扱いを期待する。加えて、しかしながら、刑法(StGB)の第206項は機能や性能への関係だけでなく、通信インフラのセキュリティにも関係する。ここでの解釈によれば、一方的な同意が受信者から得られた場合、十分でなければならない。契約上の合意の欠如により、基本的な原則として、フィッシングメールに関して人々への更なるリスクを回避するために、受信者による推定同意が想定されなければならないだろう。特定の電子メールを迷惑メール等として扱うメールボックスプロバイダのオプションに関しては、しかしながら、これを一般的に想定することはできない。むしろ、それはドイツ国憲法(GG; 情報に関しては自己決定)の第1条と合わせて第2条から結論付けることができる。

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

The criterion "unauthorized" has a twin function.[44] 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).[45]

Whether in addition general grounds for justification, such as Section 34 of the Criminal Code (StGB), could apply is disputed.[46] 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).[47] 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.[48]

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

[44] Karlsruhe Upper Regional Court 1 Ws 152/04 para. 23
[45] Fischer, 58th edition, Section 206 para. 9
[46] Fischer, 58th edition, Section 206 para. 9
[47] Fischer, 58th edition, Section 206 para. 9
[48] Karlsruhe Upper Regional Court 1 Ws 152/04 para. 25

受信者は通常、このような電子メールをどのように扱いたいか、彼自身/彼女自身で決定したい。つまり、彼自身/彼女自身でそれらを読むか、それらを無視するか、または迷惑メールとして宣言して"ゴミ箱"へ移動したい。電子メールがそれぞれの受信者にとって迷惑メールであるかどうかの評価は受信者が個々に評価する可能性がある。実際には、電子メールがそれぞれの受信者にとって迷惑メールであるかどうかの評価は受信者の定期的な仕事である。これは、しかし、情報に関して自己決定する権利には影響ない。

bb) 正当化するための他の理由
"不正"の基準は双子の機能を有している。同意に加えて、正当化の一般的な根拠は犯罪の要素を排除するために適用することができる。しかし、法的規制に記載されている同意文書だけが考慮され、電気通信法(TKG)の第88項Ⅲに明示される電気通信プロセスを参照することに注目すべきである。

ここでは、任意の割合で、刑事訴訟法(StPO)の規制が適用される。刑事訴訟法(StPO)の第99項、第100項、第100a項、第100b項、第100g項、第100h項、第100i項、第101項に対する有効な判決に基づき、刑事訴訟当局への通信コンテンツの送信が行われる。刑法(StGB)の第34項のように正当化のために一般的な根拠を加えて適用できるかどうかが係争になる。カールスルーエ上級地方裁判所の意見では、電気通信法(TKG)の第88項(3)第3節の枠組みを超える特定のケース集合が存在すれば正当化するための一般的な根拠を適用することは理解される。特定の状況では、電子メールの流布により電気通信およびデータ処理システムに故障や被害を与える原因になる場合、さらに影響を受ける当事者のためにフィッシング被害を排除できないできない場合、電子メールを配信しない、またはフィルタリングすることは正当化されるかもしれない。

ここでは、既に上記で詳細に提示した議論が再利用されることがある。

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).[49]

However, a justification can also occur here through presumed consent[50], 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.

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

2.データの変更 - 刑法(StGB) 第303a項

罰則の可能性は刑法(StGB)の第303a項(1)の改変に基づき発生する可能性がある。刑法(StGB)の第303a項はデータを処分する権利を有する当事者の利益を保護する。

電子メールが規制されている場合に法定犯罪が関連する。刑法(StGB)の第206項(2)第2号の記載を参照することができる。

しかし、刑法(StGB)の第206項(2)第2号における上述の原則を参照することで、推定同意を経て正当化できる可能性がある。

結論: 刑法の観点においては、刑法(StGB)の第206項および第303a項の両方が満たされる。しかし、罰則の可能性の排除は第一にフィッシングメールに関する受信者の推定同意に基づき考慮され、第二に詐欺狙いからの受信者の保護および最優先の電気通信のセキュリティの維持による受信者の利益保護のような正当化のための一般的な根拠が考慮される。

WE ARE SHAPING THE INTERNET.

C. Overall result and recommendations

1. The implementation of DMARC is consistent with German law, 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.

C. 全体の結論と提言

1. DMARCの実装は規制を考慮してドイツ法と整合性が取れており、いくつかは考慮すべきである。

集約レポートの法的実施は容易に実行することができるのに対して、失敗レポートの便宜的な実装はデータ保護法のもとでかなりの疑問に直面している。

詳細:

a) 集約レポートの場合

集約レポートの通信はデータ保護法上の理由から疑問である。:
法的な観点からレポートに含まれる送信元IPアドレスは個人データに分類され、したがって連邦データ保護法の要件の対象となる。
したがって、DMARC手順の枠組みにおける集約レポートの利用は、それに含まれるレポートデータは基本的に送信しなくても良いことを意味し、法律で許可される枠組みの中だけで行われても良い。すなわち、スパムやフィッシングを絞り込む、および比例の原則を維持しながら通信システムを保護するためである。
便宜的な匿名化が行われるべきである。 - 可能かつ合理的に。

b) 失敗レポートの場合

集約レポートと比較して、失敗レポートは個人データを多数含み、しかし、DMARCの有効利用のために必要不可欠ではない。
データ経済の原則に基づき、不正なメールの受信者の個人データが送信されるのを回避するために、緊急で編集に頼ることを推奨する。これらのデータは電子メールの件名と本文、受信者のEメールアドレスが必須で含まれる。

WE ARE SHAPING THE INTERNET.

2. Finally, some recommendations need to be given:

a) In order to exclude misuse with regard to the receipt of reports,[51] 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.

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

2. 最後に、いくつかの推奨事項について:
a) レポートの受信に関する不正使用を排除するため、RFC7489 7.1章に準拠して、特定のレポート受信者が実際に認証され、データの受信を希望していることを保証するため、認証および検証システムが実装される。外部のレポート用アドレスが推奨され、可能であればレポートをDMARCポリシードメインへ配信し、その後、外部のレポート用アドレスへ転送することが推奨される。

b) 加えて、受信者はEメールの代替的なアプローチについて通知され、特にスパムメールに関して決定する権限が与えられるべきである。いずれにせよ、データを処分する権限に関する手順が規定されるべきである。これは一般的な用語とISPの取引条件またはDMARCガイドラインで行われるべきである。