BESCHWERDE NACH ARTIKEL 77(1), 80(1) DSGVO
noyb Aktenzahl: C-027

A. SACHVERHALT

1. Verantwortlicher/ Auftragsverarbeiter

Diese Klage richtet sich gegen Amazon Europe Core SARL, Amazon EU SARL, Amazon Services Europe SARL und Amazon Media EU SARL, jeweils mit der Adresse 38 Avenue John F. Kennedy L-1855, Luxemburg, sowie gegen Amazon Digital Germany GmbH, Domagkstr. 28, 80807 München (zusammen „*Amazon*"), insoweit jedes Unternehmen, einzeln oder gemeinsam, als Verantwortlicher für die Gewährung der Sicherheit der Verarbeitung gilt.

2. Betroffener/Beschwerdeführer

Die betroffene Person ist Bertrand Dahi („*Beschwerdeführer*"). Herr Dahi ist ein Verkäufer auf dem Amazon Marketplace Service mit einem Konto unter folgender E-Mail-Adresse: kontakt@eichenhain.com.

Der Beschwerdeführer hat uns (den gemeinnützigen Verein *noyb* - European Centre for Digital Rights) beauftragt, ihn gemäß Artikel 80 (1) DSGVO (***Anhang 1 - Vertretungsvertrag***) zu vertreten.

3. Fakten

Der Amazon Marketplace ist eine E-Commerce-Plattform, die Amazon gehört und von Amazon betrieben wird. Es ermöglicht Drittanbietern (d.h. Nicht-Amazon-Anbietern), neue oder gebrauchte Produkte an Amazon-Nutzer auf dem von Amazon verwalteten Online-Marktplatz zu verkaufen.

Verkäufer können mit Kunden über den „*Käufer-Verkäufer-Postfach*" von Amazon kommunizieren. Um mit dem Kunden über das Käufer-Verkäufer-Postfach zu kommunizieren, muss ein Verkäufer sein Amazon-Konto besuchen (Abschnitt „*Seller Central*"), eine Nachricht verfassen und auf die Schaltfläche „*E-Mail senden*" klicken (***Anhang 2 - Screenshot des Messaging Service***).

COMPLAINT UNDER ARTICLE 77(1) GDPR

A. FACTUAL BACKGROUND

1. Controller/Respondent

This complaint is filed against Amazon Europe Core SARL, Amazon EU SARL, Amazon Services Europe SARL, and Amazon Media EU SARL, all located at 38 avenue John F. Kennedy L-1855, Luxembourg, and Amazon Digital Germany GmbH, Domagkstr. 28, 80807 Munich (together "*Amazon*"), in so far as each, singly or jointly, is the responsible controller or processor to ensure security of processing.

2. Data subject/Complainant

The data subject is Bertrand Dahi ("*Complainant*"). Mr Dahi is a seller on the Amazon Marketplace service with an account under the following email address: kontakt@eichenhain.com.

The complainant has mandated us (the non-profit association *noyb* – European Centre for Digital Rights) to represent him pursuant to Article 80(1) GDPR (***Attachment 1 – Representation agreement***).

3. Facts

Amazon Marketplace is an e-commerce platform owned and operated by Amazon. It enables third-party (i.e. non-Amazon) sellers to sell new or used products to Amazon users on the online marketplace managed by Amazon.

Sellers can communicate with customers through Amazon's "*Buyer-Seller Messaging Service*". In order to communicate with the customer through the Buyer-Seller Messaging Service, a seller needs to visit their Amazon account (the "*Seller Central*" section), draft a message, and click on the button "*Send email*" (***Attachment 2 – Screenshot of the Messaging Service***).

The message is delivered to the customer's Amazon inbox within the Buyer-Seller Messaging Service. A copy of the message is typically also sent to both

Die Nachricht wird innerhalb des Käufer-Verkäufer-Postfachs an die Amazon-Inbox des Kunden übermittelt. Eine Kopie der Nachricht wird in der Regel auch an die E-Mail-Adresse des Verkäufers und des Kunden gesendet, die bei Amazon registriert sind (***Anhang 3 - Käufer- und Verkäufer-E-Mail***).

Ein Verkäufer kann auch E-Mails direkt an den Kunden von seiner eigenen E-Mail-Adresse senden. Da Amazon jedoch nicht die registrierte E-Mail-Adresse des Kunden anzeigt, sondern nur eine Alias-E-Mail-Adresse, die mit den Internetdomänen von Amazon verbunden ist, wird die E-Mail über die Server von Amazon weitergeleitet.

Somit werden alle an den Kunden gesendete Nachrichten von Amazon verarbeitet, unabhängig davon, ob die Nachricht des Verkäufers aus dem Käufer-Verkäufer-Postfach oder einem externen E-Mail-Konto stammt. Wenn ein Verkäufer also eine E-Mail von seinem E-Mail-Konto an die Alias-E-Mail-Adresse des Käufers sendet, geht die Kommunikation über die E-Mail-Server von Amazon.

Die E-Mail wird mit dem Simple Mail Transfer Protocol („*SMTP*“) gesendet. Das bedeutet, dass der Nachrichteninhalt in Klartext verschickt wird. Ein analoger Vergleich dazu wäre eine normale Postkarte, die von jedermann gelesen werden kann. SMTP ist daher ein von Natur aus unsicheres Protokoll (siehe 4 unten).

Die E-Mail-Server von Amazon, wie „*retail-smtp-in-eu-1.amazon.co.uk*“, „*retail-smtp-in-eu-2.amazon.co.uk*“ und „*retail-smtp-in-eu-3.amazon.co.uk*“ (eine vollständige Liste finden Sie in ***Anhang 4***), akzeptieren keine Form der Verschlüsselung der Transportschicht. Wenn der Absender höhere Sicherheitsstandards verwendet – und Amazon auffordert, diese zu akzeptieren –, einschließlich der Verschlüsselung der Transportschicht, verweigern die Server von Amazon dies und lehnen die Verbindung ab (***Anhang 5***).

Das oben Gesagte gilt auch in umgekehrter Richtung. Wenn ein Kunde einen Verkäufer kontaktieren möchte, kann er das eingebaute Messaging-System

the seller and customer's email address as registered with Amazon (***Attachment 3 – Buyer and Seller Email***).

A seller can also send emails directly to the customer from their own email address. However, since Amazon does not show the customer's registered email address, but only an alias email address connected to Amazon's internet domains, the email is routed through Amazon's servers.

As such, all messages sent to the customer are processed by Amazon, regardless of whether the seller's message originates within the Buyer-Seller Messaging Service or external email account. Consequently, when a seller sends an email from his email account to the buyer's alias email address, the communication passes through Amazon's email servers.

The email is sent using the Simple Mail Transfer Protocol ("*SMTP*"). As such, the content of the message is sent in plain text. An analogue comparison would be a common postcard whose content can be read by anyone. SMTP is therefore an inherently insecure protocol (see 4 below).

Amazon's email servers, such as "*retail-smtp-in-eu-1.amazon.co.uk*", "*retail-smtp-in-eu-2.amazon.co.uk*" and "*retail-smtp-in-eu-3.amazon.co.uk*" (for a complete list, please refer to ***Attachment 4***), do not accept any form of transport layer encryption. If the sender uses – and requests Amazon to accept – higher security standards that include transport layer encryption, Amazon's servers refuse to do so and refuse the connection (***Attachment 5***).

The above is also true in the opposite direction. If a customer desires to reach out to a seller, they can use the dedicated built-in messaging system within the Buyer-Seller Messaging Service or send an email to the alias email address of

innerhalb des Käufer-Verkäufer-Postfachs nutzen oder eine E-Mail an die Alias-E-Mail-Adresse des Verkäufers senden. E-Mails, die an „*@marketplace.amazon.co.uk*“ (oder andere ähnliche Domains, die Amazon zur Erstellung des oben genannten Kunden-E-Mail-Alias verwendet) gerichtet werden, können nicht mit einem höheren Sicherheitsstandard als reines SMTP versandt werden (***Anhang 6***).

Obwohl Verschlüsselungsstandards heutzutage extrem einfach zu implementieren sind, erfolgt die Kommunikation *mit den* Marktplatz-Servern von Amazon nach unserem Kenntnisstand über das grundlegende SMTP-Protokoll ohne zusätzliches Verschlüsselungsprotokoll, wie beispielsweise Transport Layer Security (TLS) (***Anhang 7***).

4. SMTP - ein altes, unsicheres Übertragungsprotokoll

Die Hauptfunktion des Simple Mail Transfer Protocol besteht darin, E-Mails zu übertragen. Dazu verwendet das Protokoll eine Reihe von vordefinierten Befehlen und Antworten, die den Transfer der E-Mail zwischen Servern authentifizieren und steuern (mindestens ein Sende- und ein Empfangsserver, wie in *Abbildung 1* dargestellt). Der Dialog der Befehle und Antworten wird als „*SMTP-Konversation*“ bezeichnet.

Im vorliegenden Fall, wenn ein Benutzer auf die Schaltfläche „*E-Mail senden*“ klickt, sendet der Amazon-Server die Nachricht an den Benutzer und bestimmt, wohin die E-Mail geleitet werden soll. Wenn ein Kunde beispielsweise ein Google-E-Mail-Konto hat, ruft Amazon eine Liste der akzeptierenden Server von diesem Anbieter ab (z.B. *smtp.google.com*) und baut die *SMTP-Konversation* auf.

the seller. Any emails addressed to “*@marketplace.amazon.co.uk*” (or other similar domains that Amazon uses to create the above-mentioned customer email alias) cannot be sent using any higher security standard than pure SMTP (***Attachment 6***).

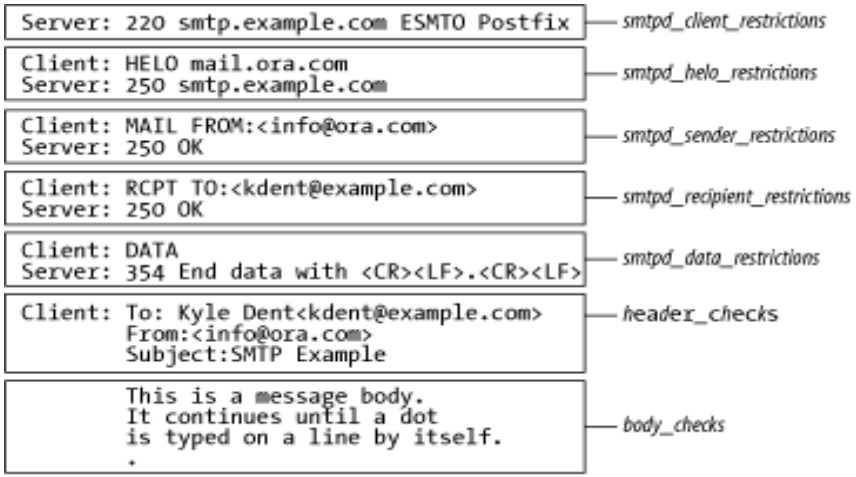
Although encryption standards are nowadays extremely easy to implement, to our knowledge communications sent *to* Amazon’s marketplace servers are done – or forced to be done – via the basic SMTP protocol without any additional encryption protocol, such as Transport Layer Security (TLS) (***Attachment 7***).

4. SMTP – an old, insecure transfer protocol

The Simple Mail Transfer Protocol’s main function is to transfer email. To do so, the protocol uses a set of predefined commands and responses that authenticate and direct the transfer of the email between servers (which will be at least one sending and one receiving server, as demonstrated in *Graph 1*). The dialogue of commands and responses is called the “*SMTP conversation*”.

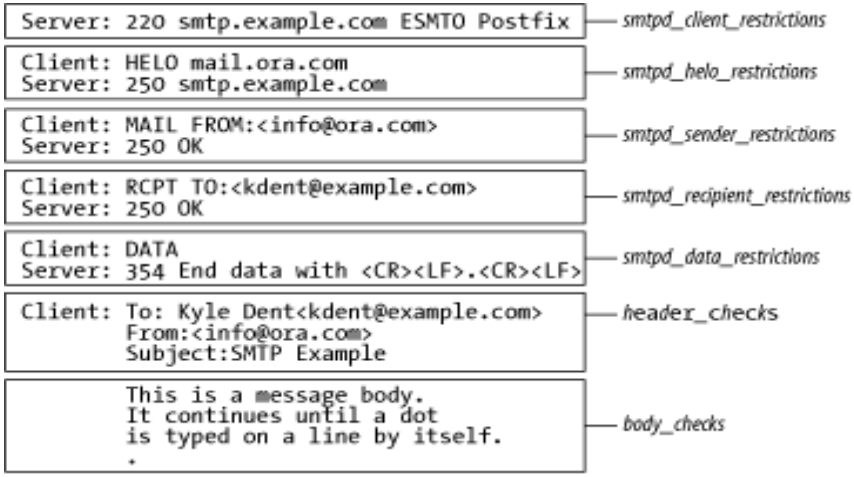
In the present case, when a user hits the “*Send email*” button, Amazon’s server sends the message for the user and determines where to direct the email. For example, if a customer has a Google email account, Amazon retrieves a list of accepting servers from that provider (say, *smtp.google.com*) and establishes the *SMTP conversation*.

Abbildung 1 - Quelle: https://flylib.com/books/en/2.262.1/client_detection_rules.html



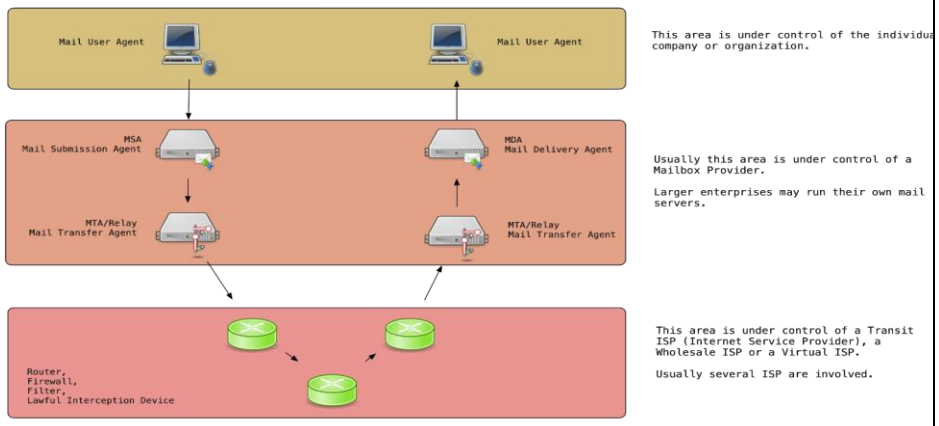
Die Verwendung von nativem SMTP bedeutet, dass alle in *Grafik 1* dargestellten Elemente (d.*h.* Server, E-Mail-Adressen, Betreff, Nachrichtentext und andere Metadaten) in Klartext gesendet werden. Dies wäre kein Problem, wenn Client und Server die einzigen beiden Akteure in der Kommunikationskette wären. Ein solcher einfacher bilateraler Dialog ist jedoch nur theoretisch und muss im Kontext der hochgradig artikulierten Struktur des Internets erklärt werden.

Graph 1 – Source: https://flylib.com/books/en/2.262.1/client_detection_rules.html



The use of native SMTP implies that all the elements showed in *Graph 1* (*i.e.* servers, emails addresses, subject, body of the message, and other metadata) are sent in plain-text. This would not be an issue if client and server above were the only two actors in the communication chain. However, such simple bilateral dialogue is only theoretical and needs to be explained in the context of the highly articulated structure of the internet.

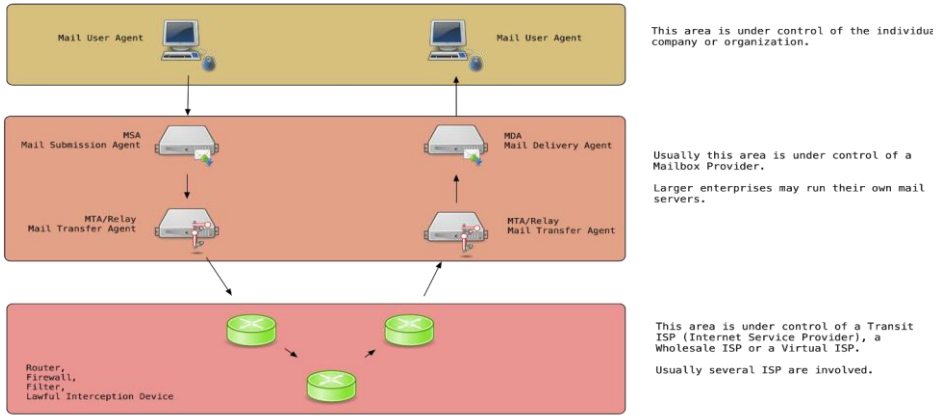
Grafik 2



Obwohl stark vereinfacht, beschreibt *Grafik 2* SMTP-Interaktionen über das Internet. Jede Schicht repräsentiert die Akteure, die am Senden und Weiterleiten der E-Mail an den Empfänger beteiligt sind. Die grafischen Symbole stellen die notwendigen elektronischen Verarbeitungsvorgänge dar, die beim Senden der E-Mail an den richtigen Empfänger erforderlich sind. Jedes Symbol repräsentiert einen sogenannten „Node“. Die schwarzen Pfeile zwischen den Nodes bis zum letzten MTA/Relay-Symbol basieren auf SMTP und bilden die SMTP-Konversation. Die unterste rote Schicht verdeutlicht die Existenz einer Vielzahl von Akteuren, die, wie im obigen Beispiel dargestellt, weder zu Amazon noch zu Google gehören. Dieses Teilnetzwerk wird von Dritten betrieben, über die weder Amazon noch Google (dem Mailanbieter des Beschwerdeführers) eine Kontrolle ausüben können.

Der Klartextcharakter jeder SMTP-Kommunikation bedeutet, dass diese externen Parteien uneingeschränkten Zugang zum Inhalt der Kommunikation haben, was *unter anderem* ihre Integrität und Vertraulichkeit (Art. 5(1)(f)

Graph 2



Although in a simplistic way, *Graph 2* describes SMTP interactions over the Internet. Each layer represents the actors involved in sending and routing the email to the recipient. The graphic icons represent necessary electronic processing operations involved in sending the email to the correct recipient. Each icon represents a so-called “node”. The black arrows between the nodes until the last MTA/Relay icon rely on SMTP and form the SMTP conversation. The lowest red layer highlights the existence of a plurality of actors which, sticking to the example above, belong neither to Amazon nor to Google. This sub-network is operated by third parties that neither Amazon nor Google (the mail provider of the data subject) are able to exercise any control over.

The plain-text nature of every SMTP communication means that such external parties have full access to the content of the communications, threatening *inter alia* their integrity and confidentiality (Art 5(1)(f) GDPR). The consequent risks

DSGVO) gefährdet. Die daraus resultierenden Risiken sind vielfältig: Änderung des Inhalts der gesendeten E-Mail; unbefugtes Abfangen und Offenlegen von Informationen an andere Personen als die benannten Empfänger; Analyse durch andere Länder, wenn der Netzwerkverkehr durch dieses Land geleitet wird; Man-in-the-Middle-Angriffe sowie andere Risiken (***Anhang 8***).

Aus diesen Gründen hat sich SMTP im Laufe der Jahre kontinuierlich verbessert. So wurde beispielsweise 2002 das Protokoll um TLS-Verschlüsselung erweitert, um „*SMTP-Agenten die Möglichkeit zu* geben*, ihre Kommunikation ganz oder teilweise vor Lauschern und Angreifern zu schützen*" (RFC 3207). Die aktuelle Empfehlung (*RFC 7672*) verbessert die TLS-Verschlüsselung gegen verschiedene Sicherheitsbedrohungen. Ab 2018 gilt die Verwendung von SMTP ohne TLS-Erweiterung als obsolet (RFC 8314 - ***Anhang 9***).

Marketplace ist einer der größten Online-Märkte der Welt. Es werden täglich Millionen von Transaktionen auf dem Marktplatz mit den dazugehörigen E-Mails, Auftragsbestätigungen, Auftragsanfragen und Stornierungen durchgeführt (***Anhang 10***). Das Fehlen jeglicher Verschlüsselungsstandards auf den Servern von Amazon Europe führt zu einer massiven Anzahl von ungesicherten und ungeschützten Kommunikationen.

B. RECHTLICHE ANALYSE

1. Rechtsverletzungen

Wie gemäß § 24(2) DSG 2018 erforderlich, behauptet der Beschwerdeführer einen Verstoß gegen seine Grundrechte auf Achtung des Privatlebens und den Schutz personenbezogener Daten (Artikel 7 und 8 CFR und §1 DSG) sowie gegen die Artikel 24, 25 und 32 DSGVO.

are many: changing the content of the sent email; unauthorized interception and disclosure of information to persons other than the designated recipients; analysis by other countries when the network traffic is routed through that country; Man-in-the-Middle attacks, as well as other risks (***Attachment 8***).

For these reasons, SMTP has undergone continuous improvements over the years. For example, in 2002 the protocol was extended with TLS encryption to give "*SMTP agents the ability to protect some or all of their communications from eavesdroppers and attackers*" (RFC 3207). The current recommendation (*RFC 7672*) improves TLS-encryption against various security threats. As of 2018, the use of SMTP without a TLS extension is considered obsolete (RFC 8314 - ***Attachment 9)***

Marketplace is one of the world's largest online market. Every day millions of transactions are carried out in the marketplace with the associated emails, order confirmations, order queries and cancellations (***Attachment 10***). The lack of any encryption standards on Amazon Europe's servers leads to a massive amount of unsecured and exposed communications.

B. LEGAL ANALYSIS

1. Violated rights

As required by § 24(2) Austrian Data Protection Act 2018, the Complainant alleges the violation of his fundamental right to privacy and data protection (Articles 7 and 8 CFR and § 1 DSG) as well as Articles 24, 25, and 32 GDPR.

2. Die DSGVO gilt für den Fall

Die über die Server von Amazon gesendeten E-Mails enthalten Informationen wie IP-Adresse und E-Mail-Adresse des Benutzers, Vorname, Nachname, Kaufdetails sowie andere Metadaten, die im Header der Nachricht enthalten sind.

Diese Informationen erfüllen die Definition von personenbezogenen Daten gemäß Artikel 4(1) DSGVO: *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind".*

Die Gesamtabwicklung der E-Mails und der enthaltenen personenbezogenen Daten durch Amazon, insbesondere die Übertragung von *Node 1* (z.B. "*retail-smtp-in-eu-1.amazon.co.uk*") auf *Node 2* (hypothetisch "*interchange-smtp-panama.com.pa"),* erfüllt auch die Definition der *Verarbeitung* nach Artikel 4 Absatz 2 DSGVO.

3. Die Pflicht zur Datensicherheit nach der DSGVO

Integrität und Vertraulichkeit ist eines der wichtigsten Prinzipien des Datenschutzes. Der Verantwortliche muss personenbezogene Daten *„in einer Weise verarbeite*(n), *die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen"* (Artikel 5(1)(f) DSGVO).

Alle Datenverarbeitungssysteme „*müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der*

2. The GDPR applies to the case

The emails sent via Amazon's servers contain information such as users' IP and email address, name, surname, purchase details as well as other metadata included in the header of the message.

This information fulfils the definition of personal data set forth by Article 4(1) GDPR: "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

The overall handling of the emails and the contained personal data by Amazon, and in particular the transfer from *Node 1* (say, "*retail-smtp-in-eu-1.amazon.co.uk*") to *Node 2* (hypothetically, "*interchange-smtp-panama.com.pa"*), also fulfils the definition of *processing* under Article 4(2) GDPR.

3. The security obligation under the GDPR

Integrity and confidentiality is one of the key principles of data protection. Controllers and processors must ensure "*appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*" (Article 5(1)(f) GDPR).

All data processing systems "*shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number*

Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden“ (Artikel 25 (2) DSGVO). Insbesondere sind die Verantwortlichen dazu verpflichtet, „*geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“* (Artikel 32(1) DSGVO), beispielsweise durch Verschlüsselung (Artikel 32 (1) (a) DSGVO). Gemäß Artikel 24 (1) DSGVO sollen *„Maßnahmen erforderlichenfalls überprüft und aktualisiert“ werden.*

Dies impliziert die Durchführung einer ersten Datenschutz-Folgenabschätzung – sowie wirksamer laufender Compliance-Programme – zur Bewertung von, insbesondere, "*Herkunft, Art, Besonderheit und Schwere dieses Risikos*" (Kelleher, „EU Data Protection Law“, Bloomsbury Professional 2018, S. 285).

Das Ergebnis der Bewertung sollte bei der Festlegung der zu erlassenden Sicherheitsmaßnahmen berücksichtigt werden. Eine angemessene Umsetzung von Artikel 32 DSGVO würde zunächst eine Liste aller möglichen Sicherheitsmaßnahmen zur Verringerung der identifizierten Risiken aufstellen, um dann die am besten geeignete Maßnahme unter Berücksichtigung von Faktoren wie Durchführungskosten, Art und Kontext der Verarbeitung auswählen.

4. Amazon hat keine geeignete Sicherheitsmaßnahmen ergriffen

Täglich werden SMTP E-Mails in Klartext zwischen Verkäufer und Kunden des Amazon Marketplace verschickt. In bestimmten Fällen enthalten diese Meldungen besondere Datenkategorien gemäß Artikel 9 DSGVO. Dies kann beispielsweise der Fall sein, wenn ein Käufer eine politische Broschüre, ein religiöses Gut oder ein Buch über eine schwere Krankheit kauft.

Solche unverschlüsselten Mitteilungen können sowohl von Einzelpersonen als auch von ausländischen Regierungen jederzeit abgefangen werden, mit potenziellem Schaden für die Nutzer (siehe Anhang 8). Als Reaktion darauf hätte die Risikobewertung von Amazon – falls vorhanden – eine geeignete Sicherheitsmaßnahme identifizieren müssen, die ein solches rechtswidriges Abfangen verhindert.

of natural persons” (Article 25(2) GDPR). Specifically, controllers and processors are obliged to “*implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk”* (Article 32(1) GDPR), for example through encryption (Article 32(1)(a) GDPR). Under Article 24(1) GDPR, “*[t]hose measures shall be reviewed and updated where necessary*”.

The above implies the carrying-out of an initial data protection impact assessment – as well as effective ongoing compliance programs – to evaluate, in particular, “*the origin, nature, particularity and severity of that risk*” (Kelleher, ‘EU Data Protection Law’, Bloomsbury Professional 2018, p. 285).

The outcome of the assessment should be taken into account when determining which security measures shall be adopted. An adequate implementation of Article 32 GDPR would first identify a list of all possible security measures to reduce the identified risks to then select the most “appropriate” measure, taking into account factors such as costs of implementation, nature and context of the processing.

4. Amazon failed to implement appropriate security measures

Each day, SMTP plain-text emails are circulated among Amazon Marketplace sellers and customers. In certain cases, these messages will contain special categories of data under Article 9 GDPR. This may be, for example, because a buyer purchases a political pamphlet, a religious good, or a book focused on a serious disease.

Such unencrypted communications can be intercepted at any time by both individuals and (foreign) governments with potential damage for the users (see Attachment 8). In response to this, Amazon’s risk assessment – if any – should have identified an appropriate security measure preventing such unlawful interception.

SMTP ist offensichtlich nicht die Lösung. Wie oben gezeigt, ist SMTP nur ein technisches Mittel zur Kommunikation von Informationen zwischen verschiedenen Servern. Sie ermöglicht diese spezielle Art der Verarbeitung (Plaintextübertragung von E-Mails), ist aber keine Sicherheitsmaßnahme. Eine Sicherheitsmaßnahme ist eine ergänzende Maßnahme, die geeignet ist, die mit der Verarbeitung verbundenen Risiken zu reduzieren.

Im vorliegenden Fall würde die TLS-Verschlüsselung das Risiko eines rechtswidrigen Zugriffs auf die übertragenen personenbezogenen Daten erheblich reduzieren (siehe Anhang 9). Eine solche Maßnahme ist nicht nur effektiv, sondern auch extrem einfach umzusetzen. Wie das Information Commissioner's Office des Vereinten Königreichs bereits klargestellt hat, *ist* "*[e]ncryption eine weit verbreitete Maßnahme mit relativ niedrigen Implementierungskosten. Es gibt eine große Vielfalt an Lösungen*" (*Anhang 11*).

Mit anderen Worten, ist Verschlüsselung (z.B. **TLS**) die geeignete Maßnahme zur Sicherung personenbezogener Daten während der Übertragung.

In diesem Zusammenhang hat die Artikel-29-Datenschutzgruppe bekräftigt, dass eine "*starke und effiziente Verschlüsselung*" nicht nur angemessen ist, sondern auch "*eine Notwendigkeit, um den Schutz des Einzelnen im Hinblick auf die Vertraulichkeit und Integrität seiner Daten zu gewährleisten, die die elementare Grundlage der digitalen Wirtschaft bilden"* [Hervorhebung hinzugefügt].

"Die Sicherung personenbezogener Daten während der Übermittlung und im Ruhezustand ist ein Eckpfeiler des Vertrauens, das wir alle für digitale Dienste benötigen [...] *[G]eeignete Algorithmen bieten eine angemessene Garantie dafür, dass Aktivitäten wie der Online-Kauf von Waren* [...] *sicher durchgeführt werden können. Ohne Verschlüsselung kann die Privatsphäre und Sicherheit des Einzelnen jedes Mal beeinträchtigt werden, wenn er diese alltäglichen Aktivitäten durchführen möchte"*[Hervorhebung hinzugefügt].

Clearly, SMTP is not the answer. As shown above, SMTP is only a technical means for communicating information between different servers. It enables this specific type of processing (plain text transfer of emails) but is not a security measure. A security measure is a supplementary action able to reduce the risks associated with the processing.

In the present case, TLS encryption would significantly reduce the risks of unlawful access to the personal data in transit (see Attachment 9). Such a measure is not only effective, but also extremely easy to implement. As the UK's Information Commissioner's Office already clarified, "*[e]ncryption is a widely-available measure with relatively low costs of implementation. There is a large variety of solutions available*" (***Attachment 11***).

In other words, encryption (i.e. **TLS**) is the appropriate measure to secure personal data in transit.

On this point, the Article 29 Working Party affirmed that a "*strong and efficient encryption*", is not only appropriate, but also "*a necessity in order to guarantee the protection of individuals with regard to the confidentiality and integrity of their data which are the elementary underpinning of the digital economy"* [emphasis added].

"Securing personal data in transit and at rest is a cornerstone of the trust we all need for digital services [...] *[A]ppropriate algorithms offer a reasonable guarantee that activities like buying goods online* [...] *can be done securely.* […] *Without encryption, individuals' privacy and security can be compromised every time they wish to undertake those everyday activities"* [emphasis added].

Zusammenfassend lässt sich sagen: *"Verschlüsselung ist daher absolut notwendig und unersetzlich, um eine hohe Vertraulichkeit und Integrität bei der Übertragung von Daten über offene Netzwerke wie das Internet zu gewährleisten. Diese Verschlüsselung sollte idealerweise immer die gesamte Kommunikation vom Gerät des Absenders bis zum Empfänger umfassen (End-to-End-Verschlüsselung)*" (***Anhang 12***).

Ungeachtet dessen hat Amazon entscheiden, dies nicht zu tun, entweder wegen einer fehlender Bewertung der Sicherheitsrisiken oder wegen der mangelhaften Schlussfolgerung, dass die Verwendung des reinen SMTP-Standards die Interessen von Millionen von Betroffenen schützen würde.

C. ANTRÄGE

1. Anträge zur Untersuchung

Die betroffene Person bittet Sie (oder jede andere Aufsichtsbehörde, mit der Sie gemäß Kapitel VII DSGVO zusammenarbeiten), diese Beschwerde in Übereinstimmung mit den Ihnen übertragenen Befugnissen, einschließlich Artikel 58(1)(a), (e) und (f) DSGVO, vollständig zu untersuchen, um festzustellen, ob das Folgende der Fall ist oder nicht:

(i) Der Verantwortliche hat eine erste und laufende Sicherheitsbewertung gemäß Artikel 32(1) und Artikel 24(1) DSGVO durchgeführt;

(ii) Die Verwendung von SMTP ohne jegliche zusätzliche Verschlüsselung gewährleistet ein angemessenes Sicherheitsniveau gemäß Artikel 32(2) DSGVO.

Schließlich möchten wir darum bitten, dass uns die Ergebnisse dieser Untersuchung im Rahmen dieses Verfahrens gemäß Artikel 77(2) DSGVO und das Recht auf Anhörung nach dem geltenden nationalen Verfahrensrecht zur Verfügung gestellt werden.

In conclusion, *"Encryption is therefore absolutely necessary and irreplaceable for guaranteeing strong confidentiality and integrity when data are transferred across open networks like the internet* […] *This encryption should ideally always cover the entire communication, from the device of the sender to that of the recipient (end-to-end-encryption)*" (***Attachment 12***).

Notwithstanding that, Amazon decided not to do so, either because of a lack of assessing the security risks or because of the flawed conclusion that the adoption of the mere SMTP standard would safeguard the interests of millions of data subjects.

C. APPLICATIONS

1. Request to investigate

The data subject hereby requests that you (or any other supervisory authority that you may cooperate with under Chapter VII GDPR) fully investigate this complaint, in accordance with the powers vested in you, including by Article 58(1)(a), (e) and (f) GDPR, to determine whether or not:

(i) The controller has undertaken any initial and ongoing security assessment provided for by Article 32(1) and 24(1) GDPR;

(ii) The use of SMTP with no added encryption whatsoever ensures an appropriate level of security as required by Article 32(2) GDPR.

Finally, we would like to request that the results of this investigation are made available to us in the course of this procedure, in accordance with Article 77(2) GDPR and the right to be heard under the applicable national procedural law.

2. Antrag auf Verbot der betreffenden Verarbeitungen

Wir bitten Sie (oder die zuständige Aufsichtsbehörde) ferner, die betreffenden Verarbeitungen gemäß den Ihnen übertragenen Befugnissen, einschließlich Artikel 58(2)(d) und (f) DSGVO, zu untersagen.

3. Aufforderung zur Verhängung wirksamer, verhältnismäßiger und abschreckender Geldbußen

Schließlich bitten wir Sie (oder die zuständige Aufsichtsbehörde), aufgrund der in Artikel 58(2)(i) in Verbindung mit Artikel 83 (4) (a) DSGVO vorgesehenen Befugnisse eine wirksame, angemessene und abschreckende Geldstrafe gegen den für die Verarbeitung Verantwortlichen zu verhängen, wobei zu berücksichtigen ist, dass:

i. die betroffene Person nur einer von Millionen betroffener Nutzer ist (Artikel 83(2)(a) DSGVO);
ii. der Verantwortliche vorsätzlich gegen die vom DSGVO auferlegten Sicherheitsstandards verstoßen hat und betroffene Personen gezwungen wurden, der Verwendung unverschlüsselter Kommunikation zuzustimmen;
iii. der Verantwortliche die Erklärung der Artikel-29-Datenschutzgruppe über die Notwendigkeit der Verschlüsselung personenbezogener Daten während der Übermittlung gekannt haben muss, sich aber entschieden hat, diese zu ignorieren (Artikel 83(2)(b) DSGVO);
iv. der Verantwortliche keine Sicherheitsmaßnahmen ergriffen und damit gegen Artikel 32 DSGVO verstoßen hat, obwohl er als multinationales Unternehmen umfangreiche organisatorische und technische Fähigkeiten besitzt, die Wichtigkeit der Verarbeitung klar ist, und die Umsetzung von TLS oder eines anderen geeigneten Standards äußerst einfach gewesen wäre, (Artikel 83(2)(c) DSGVO);
v. der Verantwortliche hochsensible Daten verarbeitet, einschließlich besonderer Kategorien personenbezogener Daten (Artikel 83(2)(g) DSGVO);
vi. ein vorsätzlicher, massiver und schwerwiegender Verstoß eines wichtigen Akteurs der Datenindustrie angemessen geahndet werden muss, um ähnliche Verstöße gegen die DSGVO in Zukunft zu verhindern

2. Request to prohibit the relevant processing operations

We further request that you (or the relevant supervisory authority) prohibit the relevant processing operations in accordance with the powers vested in you, including by Article 58(2)(d) and (f) GDPR.

3. Request to impose effective, proportionate and dissuasive fines

Finally, we request that you (or the relevant supervisory authority), by virtue of the powers provided by Article 58(2)(i) in combination with Article 83(4)(a) GDPR, impose an effective, proportionate and dissuasive fine against the controller, taking into account that:

i. the data subject is only one of millions of affected users (Article 83(2)(a) GDPR);
ii. the controller wilfully and intentionally breached the security standards imposed by the GDPR and by forcing data subjects to agree to the use of non-encrypted communications;
iii. the controller must have known about the Article 29 Working Party Statement on the necessity of encrypting personal data in transit but chose to ignore them (Article 83(2)(b) GDPR);
iv. the controller chose not to adopt any security measure thus violating Article 32 GDPR, despite its vast organizational and technical capabilities as a multinational company, the significance of the processing and the extremely easy implementation of the TLS or other appropriate standard, (Article 83(2)(c) GDPR);
v. the controller processes highly sensitive data, including special categories of personal data (Article 83(2)(g) GDPR);
vi. a wilful, massive and profound violation by a major player within the data industry must be adequately sanctioned to prevent similar violations

und die Achtung der Rechte von betroffenen Personen im Rahmen des neuen Datenschutzrechts sicherzustellen ist.

Nach unseren Informationen lag der Umsatz der Amazon-Gruppe, zu der Amazon gehört, im Geschäftsjahr 2018 bei rund 232 Milliarden US-Dollar (rund 212 Milliarden Euro). Die mögliche Höchststrafe nach Artikel 83(4)(a) DSGVO, bemessen auf 2 % des weltweiten Umsatzes, würde demnach etwa 4,24 Mrd. € betragen.

D. SONSTIGES

1. Englische Übersetzung

Nachdem voraussichtlich verschiedene Aufsichtsbehörden mit dieser Beschwerde befasst sein werden, haben wir uns erlaubt, diese Beschwerde mit einer informellen englischen Übersetzung einzubringen. Für den Fall einer Abweichung zwischen den Übersetzungen gilt die deutsche Version, weil wir bei der gewählten Datenschutzbehörde gesetzlich verpflichtet sind, auf Deutsch einzubringen.

2. Kontaktdaten

Wir sind jederzeit gerne für Rückfragen faktischer oder rechtlicher Natur behilflich, die Sie für die Bearbeitung dieser Beschwerde benötigen sollten. Bitte kontaktieren Sie uns unter legal@noyb.eu oder +43 660 2678622.

Wien, 18.2.2020

Unterschrift

SIGNATURE INFORMATION	**Signatory**	Mag. Maximilian Gabriel Ferdinand Schrems
	Date/Time-UTC	2020-02-18T21:46:53+01:00
	Verification	Information about the verification of the electronic signature can be found at: https://www.signaturpruefung.gv.at
Note	This document is signed with a qualified electronic signature. According to Art. 25 para. 2 of the Regulation (EU) No 910/2014 of 23. July 2014 ("eIDAS-Regulation") it shall have the equivalent legal effect of a handwritten signature.	

of the GDPR in the future, and to ensure respect of the data subjects' rights under the new data protection acquis.

According to our information the revenue of the Amazon Group, to which Amazon belongs, was about $ 232 billion (about € 212 billion) in the fiscal year 2018. The possible maximum fine under Article 83(4)(a) GDPR, based on 2% of the worldwide revenue, would accordingly be about 4.24 billion.

E. OTHER

1. English translation

As different supervisory authorities will most likely deal with this complaint, we have taken the step to provide an informal English translation of this complaint. If there is any conflict in the translations, the German version should prevail because the law requires us to file this complaint with selected supervisory authority in German.

2. Kontaktdaten

We are happy to assist you with any further factual or legal details you may require to process this complaint. Please contact us at legal@noyb.eu or at +43 660 2678622.

Vienna, 18.2.2020

Signature