noyb

Opening Pandora's Box:

How companies addressed our questions about their international data transfers after the CJEU's ruling in C-311/18 - Schrems II

List of Companies

Summary:

In the wake of the CJEU's judgment in C-311/18 *Schrems II* on EU-US data transfers, the *noyb* team and some of its members sent emails to numerous companies that transfer the data of Europeans to the US. In these emails, we requested information that any user has a right to receive under Articles 12 to 15 of the GDPR, or under the relevant provisions in the so-called "Standard Contractual Clauses" (SCCs) or "Binding Corporate Rules" (BCRs).

Questions sent to companies:

Dear Sir/Madam,

I am one of your customers. In accordance with Articles 12, 13, 14 and 15 of the GDPR, I make the following requests:

- *Do you transfer data outside of the EU? If yes, to which countries?*
- *What is the legal basis relied on for each transfer (e.g. adequacy decision, SCCs, BCRs, derogations...)? If you used SCCs or BCRs, please provide a copy of the SCCs or BCRs used for each transfer.*
- *If you send personal data to the US, do any of your partners fall under 50 USC §1881a ("FISA 702") or provide data to the US government under EO 12.333?*
- *If you send personal data to the US, which technical measures are you taking so that my personal data is not exposed to interception by the US government in transit?*

Please reply within one week as the GDPR requires you to reply 'without undue delay'. This is a simple request that does not require extensive analysis. Further identification beyond my email does not seem necessary given that I do not demand a copy of my personal data. Should you require any further information, please do not hesitate to contact me.

Regards,

XXX

The questions were asked by various users of these services in different languages between 27 July and 24 September 2020, and the replies were countinously monitored. It may be that some controllers have issued more specific statements about their data transfers by now, but have not yet communicated these updates to us.

Vienna, 25. 9. 2020

Airbnb	No response to this request so far.
Data Subject 1	**Request from data subject:** *Dear Sir/Madam,* *I am one of your customers. In accordance with Articles 12, 13, 14 and 15 of the GDPR, I make the following requests:* • *Do you transfer data outside of the EU? If yes, to which countries?* • *What is the legal basis relied on for each transfer (e.g. adequacy decision, SCCs, BCRs, derogations...)? If you used SCCs or BCRs, please provide a copy of the SCCs or BCRs used for each transfer.* • *If you send personal data to the US, do any of your partners fall under 50 USC §1881a ("FISA 702") or provide data to the US government under EO 12.333?* • *If you send personal data to the US, which technical measures are you taking so that my personal data is not exposed to interception by the US government in transit?* *Please reply within one week as the GDPR requires you to reply 'without undue delay'. This is a simple request that does not require extensive analysis. Further identification beyond my email does not seem necessary given that I do not demand a copy of my personal data. Should you require any further information, please do not hesitate to contact me.* *Regards,* **No response from controller.**

Amazon	Different answers were provided to different data subjects.
Data Subject 1	**Response from controller:** Dear XXXXX, Thank you for your query. The email address you contacted us at (PrivacyShield@amazon.com) is still valid. We are aware of the recent judgment of the Court of Justice of the European Union invalidating the EU – U.S. Privacy Shield, and are actively looking into its implications. We previously relied on a several legal mechanisms, including the U.S.-EU Privacy Shield, for our transfers of personal data out of the European Economic Area. However, even before the judgment, our primary mechanism for transfers to the US was not the Privacy Shield, but the Standard Contractual Clauses (SCCs). We can assure you we continue to maintain all of our commitments under the U.S.-EU Privacy Shield with respect to data transferred under that mechanism. In addition, as stated in our Privacy Notice, whenever we transfer personal information to countries outside of the European Economic Area in the course of sharing information as set out above, we will ensure that the information is transferred in accordance with this Privacy Notice and as permitted by the applicable laws on data protection. We also take a range of technical and organizational measures to keep your data secure, including when transferred. We work to protect the security of your information during transmission by using Secure Sockets Layer (SSL) software, which encrypts information you input. In addition, Amazon does not disclose customer information in response to government demands unless we're required to do so to comply with a legally valid and binding order. Unless prohibited from doing so or there is clear indication of illegal conduct in connection with the use of Amazon products or services, Amazon notifies customers before disclosing content information. Thank you and best regards,

Data Subject 2	**First response from controller:** Guten Tag, XXXXX XXXXX wir prüfen das Urteil und seine Auswirkungen. Sie finden mehr Informationen zur Sicherheit und Schutz Ihrer Daten hier: https://www.amazon.de/privacy Freundliche Grüße, --- **Reply from data subject:** Guten Tag! Danke für Ihre Antwort. Es freut mich dass sie das Urteil prüfen, aber meine Frage war sehr klar: * An welche Unternehmen in den USA übermitteln Sie meine Daten? * Welche Rechtsgrundlage(n) nutzen Sie hierfür? Ich bitte um Antwort bis Freitag, XX. XX. XXXX, andernfalls würde ich davon ausgehen, dass Sie mein Recht auf Information und Auskunft schlichtweg ignorieren. In diesem Fall wäre ich gezwungen eine Beschwerde bei der zuständigen Aufsichtsbehörde einzubringen. Mit besten Grüßen, XXXXX --- **Subsequent response from controller:** Guten Tag, XXXXX herzlichen Dank für Ihr Schreiben an Amazon.de. Da Sie eine zweite E-Mail-Adresse benutzten, möchte ich Sie zunächst auf eine Sicherheitsmaßnahme aufmerksam machen: Aus Datenschutzgründen senden wir Informationen, die Ihr Kundenkonto bei uns betreffen, lediglich an diejenige E-Mail-Adresse, mit der Sie sich bei uns einloggen. Daher schicke ich meine Antwort an Ihre bei Amazon.de gespeicherte E-Mail-Adresse und bitte Sie, diese für weitere Anfragen über das Kontaktformular (https://www.amazon.de/kontaktformular) auf unseren Hilfeseiten zu verwenden. Sie finden meine Antwort also unter der E-Mail-Adresse Ihres Amazon.de-Kundenkontos. Sollten Sie Ihr Kundenkonto nur über eine Mobiltelefonnummer eingerichtet haben oder die E-Mail-Adresse, mit der Sie sich bei Amazon.de angemeldet haben, nicht mehr nutzen, überprüfen Sie bitte Ihre Nachrichten im Message Center. Das Message Center können Sie in der Amazon App öffnen, in dem Sie erst auf "Mein Konto" und dann unter dem Punkt "Message center" auf "Meine Nachrichten" klicken. Auf der Amazon.de-Webseite finden Sie das Message Center unter "Mein Konto" in der Rubrik "E-Mail-Benachrichtigungen, Mitteilungen und Werbung".

	Übrigens: Sie können Informationen zu Ihren Bestellungen jederzeit online abrufen. Gehen Sie dazu einfach auf "Mein Konto" auf unserer Startseite (http://www.amazon.de/). Sollten Sie allerdings die E-Mail-Adresse, unter der Sie sich bei Ihrem ersten Amazon.de-Einkauf angemeldet haben, nicht mehr benutzen, empfehlen wir, diese durch eine aktuelle Adresse zu ersetzen. Dies ist nur über unsere Website möglich, da wir sicherstellen wollen, dass die Änderung vom Kontoinhaber selbst durchgeführt wird. Dies geht ganz einfach online über "Mein Konto" rechts oben auf unserer Website (http://www.amazon.de). Wählen Sie im Bereich "Anmelden und Sicherheit" den Link "Namen, E-Mail-Adresse oder Passwort ändern" und lassen Sie sich durch die Seiten führen. (Sie erhalten von uns eine automatische E-Mail über die Änderung.) Ich danke Ihnen für Ihr Verständnis für unsere Sicherheitsmaßnahmen.
Data Subject 3	**Response from controller:** Guten Tag XXXXX, wir prüfen das Urteil und seine Auswirkungen. Sie finden mehr Informationen zur Sicherheit und Schutz Ihrer Daten hier: https://www.amazon.de/privacy Unser Ziel: das kundenfreundlichste Unternehmen der Welt zu sein. Ihr Feedback hilft uns dabei. Freundliche Grüße XXXXX
Data Subject 4	**Response from controller:** Hello XXXXX, We are studying the judgement and its implications. You can learn more about how Amazon takes care of your data, here: https://www.amazon.de/privacy Freundliche Grüße XXXXX

American Express	Asked data subject for more information, then didn't respond further.
Data Subject 1	**Response from controller:** Dear XXXXX, Before we can proceed with your request can you please provide us with some additional information so we can locate your account: • The type of card, product or service that you have with American Express • Your registered email address with us • The country where your card was issued (if applicable) • Your country of residence

	Thank you **Reply from data subject:** Hi, 1. I have a XXXXX Credit Card 2. XXXXX 3. Card issued in XXXXX 4. XXXXX resident Please respond with the answers to my questions. Thank you! **No subsequent answer from controller.**

Apple	Claim that they rely on Standard Contractual Clauses.
Data Subject 1	**Response from controller:** Dear XXXXX, Thank you for contacting Apple's privacy team. Please accept my apologies for replying in English. Apple has made available an online service for you to understand, access and control the personal information that you store with Apple: https://privacy.apple.com Please note that not all features of this service may be available in all countries. You can find out more about this service at: https://support.apple.com/HT208501 Privacy Shield is one possible mechanism for meeting requirements regarding the transfer of personal data collected in the EU to outside the EU. We are, of course, aware that it was invalidated by the Court of Justice of the European Union in the Schrems II judgment on 16 July. However, Apple was not subscribed to Privacy Shield and, in the absence of an adequacy decision (Article 45 GDPR) or a derogation for specific situations (Article 49 GDPR), relies upon Standard Contractual Clauses for the international transfer of personal information collected in the European Economic Area, the United Kingdom and Switzerland. We are also aware of the views expressed by the Court in relation to this transfer mechanism and are studying those views together with guidance emerging from data protection authorities in Europe, including the FAQs issued by the EDPB on 24 July. Please find attached as requested a copy of a redacted version of a sample of our Model Contractual Clauses. Kind regards,

Asos	Claim that they rely on Standard Contractual Clauses, and on Microsoft as communications provider.
Data Subject 1	**Response from controller:** Hi XXXXX; Thank you for your recent email. We understand that you are interested in the transfer of customer personal data outside the EEA by ASOS. In terms of GDPR compliance, ASOS.com falls under the jurisdiction of UK law (and is therefore regulated for GDPR by the UK Information Commissioner). However, you can shop with ASOS from almost any country in the world so whilst much of our customer data is held in the UK, we do manage international transfers across the world particularly through our supply chain. Given the above, we are very cognisant of our Privacy and Data Protection obligations in respect of international transfers of personal data and our approach is to adopt EU Model Contract Clauses with our suppliers as the preferred method of protecting customer data. We have a handful of suppliers in the USA who are registered with the Privacy Shield program but these companies will also have agreed to the Model Clauses. The USA legislation you have highlighted – the Foreign Intelligence Surveillance Act (FISA) focuses on the collation of internet communication data and this means that companies such as Google are captured by the legislation. We, like thousands of EU companies, use Microsoft as our communications provider, however we elected EU storage locations for our data and you may find the attached Blog from Microsoft about the recent decision and its impact for them interesting in this regard. https://blogs.microsoft.com/eupolicy/2020/07/16/assuring-customers-about-cross-border-data-flows/ We hope that the above answers your questions. Kind regards

Blizzard	Claim that they rely on Standard Contractual Clauses.
Data Subject 1	**Response from controller:** Greetings, You have reached the Data Protection Team at Blizzard Entertainment. As mentioned in the Section 6 of Blizzard's Privacy Policy, Blizzard transfers and processes personal data in the United States where many of our central databases operate. Blizzard uses the European Commission Standard Contractual Clauses to ensure appropriate safeguards of the data and adequate rights to European residents. In accordance with article 13, 1, (f) of the GDPR, you will find a copy of the applicable SCC. The general security measures Blizzard takes are mentioned in Section 11 of the Privacy Policy, however the details of those measures could compromise the integrity and security of our systems and our consumers' personal data. I can also confirm that Blizzard does not provide data to the United States Government under EO 12,333. In addition, our understanding is that Blizzard has not received any request under FISA 702. Sincerely, The Data Protection Officer

Booking	Claim that the data sent to the accommodation provider in the US does not fall under FISA 702 or EO 12.333.
Data Subject 1	**Response from controller:** Dear XXXXX; With reference to your email received by us on XXX XXX, and our subsequent email exchange between XXX XXX and XXX XXX, we would like to inform you as follows regarding the international transfer of your personal data by Booking.com. Information on the transfer of your personal data by Booking.com We have checked our systems to assess whether Booking.com has transferred or currently transfers any personal data connected to XXXXX to recipients outside the EU. Based on our records, we confirm that we only transferred personal data relating to your email address XXXXX to a recipient outside the EU in relation to a booking you made via our platform. It concerns a transfer of relevant and necessary reservation information to XXXXXX in order to provide the services you requested and complete your reservation. The transfer of your personal data was necessary for the performance of the contract to which you were a party. Understanding that XXXXX is an accommodation provider and not an electronic communication services provider under 50 USC §1881a, we have not transferred the personal data connected to XXXXX.at to a U.S.A. based electronic communication services provider to provide you with the services you requested via us. We have no information about XXXXX providing, or not, personal data to the U.S.A. government under EO 12.333. A review of our systems indicates that the personal data connected to XXXXX held by Booking.com at the present time is not subject to data transfers outside of the EU. For completeness, should you have browsed our website or used our apps and have agreed to our use of analytical and tracking cookies, we may have collected certain personal data and have transferred this data outside of the EU in accordance with our Privacy & Cookie Statement. Booking.com, however, does not connect this data to your email address. Should you have agreed to our use of analytical and tracking cookies in the past but wish to withdraw your consent, you may amend your cookie preferences at any time via the link "Manage privacy settings" at the bottom of our website. General information on Booking.com's practices on the transfer of customer data Booking.com enables users to book travel-related services throughout the world. To complete and manage these bookings, Booking.com needs to transfer personal data of the guests to the travel service provider in the country (inside or outside the EU) where the chosen accommodation or other travel service is located. We inform our users in our Privacy & Cookie Statement that their personal data may be transferred to recipients in countries where data protection laws are not as comprehensive as those of countries within the EU. These transfers are made on the basis of adequacy decisions of the European Commission, based on contractual arrangements providing appropriate safeguards to reasonably ensure that personal data is processed in line with the laws applicable to Booking.com (including unmodified EU standard contractual clauses as can be found online) or based on another approved transfer mechanism. We take appropriate technical and organizational measures to protect personal data before and upon transferring to third party recipients. These measures include data minimization measures to ensure that only relevant and necessary personal data are transferred. For example, when a user books an accommodation located in the U.S.A., Booking.com will only transfer the information necessary for the

	completion and management of that booking with the accommodation. Furthermore, we use encryption in transit and at rest in a variety of forms. The technical and organizational measures are continually assessed and updated as necessary to ensure that personal data are adequately protected in accordance with the laws applicable to Booking.com. Of course, we are aware of the recent judgment by the EU Court of Justice regarding EU-USA personal data transfers. We are currently considering the judgment and assessing the contractual arrangements and additional safeguards in place to adequately protect the personal data transferred outside the EU, including for those limited cases where Booking.com relied on the EU-US Privacy Shield framework. We have communicated with the Autoriteit Persoonsgegevens as our lead Supervisory Authority following the judgment, and will closely follow key developments, including guidance from Supervisory Authorities and the European Data Protection Board, and will revisit where need be, our personal data processing practices in accordance with such guidance. We hope this is helpful. Kind regards,

Clevver	Encourage data subject to just delete their account.
Data Subject 1	**Response from controller:** Sehr XXXXX vielen Dank für Ihre Nachricht. Unsere Datenschutzerklärung mit allen relevanten Information finden sie unter folgendem Link: [45] https://www.clevver.io/de/datenschutzerklaerung/#german Mit freundlichen Grüßen XXXXX --- **Response from data subject:** Sehr XXXXX aufgrund Ihrer Datenschutzerklärung, habe ich ein Grund zu der Annahme, dass Sie meine persönlichen Daten illegal in die Vereinigten Staaten übermitteln. Wenn Sie personenbezogene Daten an einen US "Electronic Communication Service Provider" gemäß der Definition in 18 U.S. Code §1881(4)(b) übermitteln, oder sollten Sie sich bei solchen Übermittlungen weiterhin nach dem "Privacy Shield" vornehmen, bitte ich Sie, die Übermittlung meiner personenbezogenen Daten unverzüglich einzustellen. Bitte teilen Sie mir innerhalb einer Woche mit, dass Sie die Übertragung stoppen werden, bzw ab wann Sie dies Übermittlung stoppen. Sollten Sie weitere Informationen benötigen, zögern Sie bitte nicht, mich zu kontaktieren. Mit freundlichen Grüßen XXXXX ---

Response from controller:

Sehr XXXXX
vielen Dank Für Ihre Nachricht.

Worauf beruht denn die Annahme das wir personenbezogene Daten illegal in die Vereinigten Staaten übermitteln? Für solch eine Anschuldigung muss ja ein begründeter Verdacht vorliegen.

In der Datenschutzerklärung kann ich nichts dazu finden.

Mit freundlichen Grüßen

Response from data subject:

Sehr XXXXX,

lesen Sie doch einfach Ihre eigene Datenschutzerklärung. Teilweise wird hier Privacy Shield genannt, das aber im letzten Monat für ungültig erklärt wurde. Ich bitte die genannten Punkte zu unterbinden. Es besteht kein berechtigtes Interesse diese Dienste zu nutzen.

Response from controller:

Sehr XXXXX,

vielen Dank für Ihre Nachricht und das kopieren und einfügen unserer Datenschutzerklärung. Daraus Wird immer noch nicht ersichtlich wie es dazu kommen soll das ihre persönlichen Daten "illegal in die Vereinigten Staaten übermittelt" werden. Wir empfehlen Ihnen einfach ihren Account zu löschen. Da sie bis zum heutigen Tage die Postbox nicht genutzt haben, keine Unterlagen zur Verifizierung hochgeladen haben, bereits gekündigt und nur einen reduzierten Jahresbeitrag gezahlt haben, sollte dies die Angelegenheit beendet können.

Mit Freundlichen Grüßen

Reply from data subject:

Sehr XXXXX

Sie wollen es konkret? Bitte schön (s. Anhang). Ich fordere Sie letztmalig innerhalb von 5 Tagen auf, den illegalen Datenexport in die USA zu unterlassen. Ein berechtigtes Interesse ihrerseits besteht nicht. Selbst der Verfizierungsprozess ist mit Trackern vollgestopft, oder warum muss Google hier wissen, wer alles auf der Verfikationsseite war?

Mit freundlichen Grüßen
XXXXX

Response from controller:

Sehr XXXX

	vielen Dank für Ihre Nachricht. Wie in meiner vorherigen Mail bereits erwähnt legen wir Ihnen nah ihren Account einfach zu löschen. Er wird und wurde von Ihnen bis zum heutigen Tage nicht genutzt. Bei Ihrer Anmeldung wurden sie auf die Datenschutzerklärung verwiesen und waren damit einverstanden. Eine nachträgliche Änderung der von uns genutzten Dienste ist nicht möglich. Mit freundlichen Grüßen XXXXXXX

Coinbase	Provided a thourough answer along with copies of their Standard Contractual Clauses.
Data Subject 1	**Response from data controller:** Dear XXXXX, We are in receipt of your email seeking further information about how Coinbase transfers personal data outside the EU. As described in our Privacy Policy, which you can view online here, given your location and depending upon the services you utilize, either CB Payments, Ltd., or Coinbase UK, Ltd., both located in the United Kingdom, processes your personal data (note that certain services for EU users will be moving to our Irish entity following Brexit going into effect). These UK and Ireland based Coinbase entities transfer personal data outside the EU to Coinbase, Inc., located in the United States, which does not fall within the scope of FISA 702 as it is not an electronic communications service provider. The Coinbase entities rely on Controller-to- Processor Standard Contractual Clauses (SCCs) as the legal basis of such transfer. Pursuant to your request, a copy of the template SCCs applied in our intercompany agreements between Coinbase Inc. and Coinbase UK and CB Payments, respectively, are attached hereto. Coinbase takes extensive steps to ensure its customers personal data remains private and secure. All personal data sent from the EU to Coinbase, Inc. in the U.S. is encrypted in transit and at rest. Sensitive data is stored using bank level AES-256 encryption on our servers. In addition, all traffic goes over SSL to prevent third parties from eavesdropping on the transfer or intercepting any information. Employee access is heavily restricted and Coinbase Inc.require background checks on all employees. Coinbase Inc. provides extensive guidance to its customers on the steps they can take to keep their account information secure at: https://help.coinbase.com/en/coinbase/privacy-and-security/data-privacy/how-can-i-make-my-account-more-secure#secure-your-email Coinbase, Inc. has documented procedures for handling requests for information from law enforcement. Under these procedures, our team of specialists ensures that each request we receive is valid and verifiable and attempts to limit the scope of information requests (example here). While Coinbase, Inc. respects the legitimate interests of law enforcement agents in prosecuting criminals who abuse others and our platform, we balance that interest against our customers' privacy rights, and will push back where appropriate, even when it is inconvenient or costly to do so. Coinbase, Inc. relies on Google and Amazon for enterprise-wide services, which include storage of personal data for EU data subjects. Pursuant to the Schrems II decision, and EDPB's FAQs relating thereto, Coinbase Inc. has undertaken an analysis of the use of SCCs in relation to such transfers of EU personal data to Google and Amazon. These companies' respective policies for responding to government requests for data are available here and here. Coinbase also relies on partners like Google and Facebook for performance marketing and analytics services, though EU data subjects are opted out of such tracking by default and must affirmatively consent to such tracking via our Cookie Consent Manager. All third parties processing personal data on Coinbase's behalf undergo a robust privacy and security assessment, and execute an Article 28-compliant data protection addendum requiring the processor

	to, among other things, encrypt all personal data at rest and in transit, implement organizational, physical, technical, and administrative safeguards designed to ensure the safety, integrity, and reliability of such personal data, to notify Coinbase of any third party requests for personal data it is processing on behalf of Coinbase and liaise with Coinbase before complying with such requests, and to comply with all applicable data privacy laws and regulations. Coinbase continues to monitor closely all guidance provided by the EU in relation to the EU personal data transfer issue, and is committed to making the necessary adjustments to ensure its data protection practices are compliant with the applicable data protection laws.

Ebay	Claim that they rely both on Standard Contractual Clauses and Binding Corporate Rules.
Data Subject 1	**First response from data controller:** Sehr XXXXX vielen Dank für Ihre Nachricht. Gerne bestätigen wir hiermit den Eingang Ihrer Anfrage, die wir zeitnah und im Rahmen der gesetzlichen Fristen beantworten werden. Wir wünschen Ihnen ein schönes Wochenende und verbleiben Mit freundlichen Grüßen, --- **Second response from data controller:** Sehr XXXXX wir nehmen Bezug auf Ihre Anfrage und stellen Ihnen im Folgenden die Auskünfte entsprechend Art. 15 Abs. 1 und Abs. 2 DSGVO bereit. Im Rahmen der Erbringung unserer Leistungen übermitteln wir personenbezogene Daten auch an Empfänger in Ländern außerhalb des EWR. Eine Übersicht über die Empfänger findet sich in Ziffer 5 unserer Datenschutzerklärung. In Folge des Urteils des EuGH in der Rechtssache C-3111/18 („Schrems II-Urteil“) haben wir unverzüglich begonnen, die Maßnahmen, die wir zur Absicherung der Übermittlung personenbezogener Daten in Drittländer einsetzen, zu überprüfen. Wir arbeiten dabei eng mit den zuständigen Aufsichtsbehörden sowie unseren Partnern zusammen. Ferner beobachten wir den politischen Prozess zu diesem Thema, um unsere internen Abstimmungen an die neue Informationslage anzupassen. Höchste Priorität hat bei all diesen Maßnahmen, die Betroffenen, deren personenbezogenen Daten wir verarbeiten, bestmöglich vor Beeinträchtigungen zu schützen. Für Übermittlungen, die nicht durch einen bestehenden Angemessenheitsbeschluss der EU-Kommission abgesichert sind, verwenden wir Binding Corporate Rules (BCRs) sowie die Standardvertragsklauseln (SCC) der EU-Kommission. Die SCC sind auf der Webseite der EU-Kommission frei zugänglich. Eine Kopie der bislang verwendeten BCRs, zu denen wir derzeit auch weiter im engen Austausch mit der zuständigen Aufsichtsbehörde stehen, kann in unserem Datenschutzzentrum abgerufen werden. Zusätzlich zu diesen Schutzmaßnahmen gewährleisten wir über die von uns implementierten technischen und organisatorischen Maßnahmen (TOMs) ein hohes Niveau an Datensicherheit. Unsere TOMs umfassen insbesondere Maßnahmen zur Verschlüsselung – sowohl bei der Speicherung als auch Übermittlung – als auch Maßnahmen zum Hashing personenbezogener Daten. Dadurch begrenzen wir die Risiken für die Rechte und Freiheiten der Betroffenen im Falle eines berechtigten oder auch

	unberechtigten Zugriffs auf diese Daten durch Dritte. Ohne den entsprechenden Hashwert bzw. De-Entschlüsselungscode bleiben die Informationen für Dritte informationsleer. Die konkreten Maßnahmen bestimmen sich nach den Umständen des Einzelfalles. Dabei berücksichtigen wir insbesondere die Sensibilität der verarbeiteten Datenkategorien, die Schutzbedürftigkeit der Betroffenen sowie Art und Umfang der Verarbeitung. Unsere TOMs unterliegen dabei einer ständigen Überprüfung und Anpassung. Wir haben unverzüglich nach Veröffentlichung des Schrems II-Urteils Prozesse initiiert, um den Überarbeitungsbedarf bestehender Maßnahmen festzustellen und entsprechend umzusetzen. Zusammen mit den anderen von uns bereits ergriffenen Maßnahmen sorgt dieses Vorgehen dafür, dass wir für alle Betroffenen, deren personenbezogene Daten wir verarbeiten, ein angemessenes Schutzniveau sicherstellen können. Mit freundlichen Grüßen, --- **Response from data subject:** Guten Tag! Danke für die Nachricht unten. Nachdem ich eine „Recall"-E-Mail erhalten habe, bitte ich Sie kurz klarzustellen ob diese Antwort nun die finale ist. Schönes Wochenende! Mit besten Grüßen, XXXXX --- **Response from controller:** Hallo XXXXX, Vielen Dank für die Nachfrage. Ja, das ist die korrekte Antwort. Beste Grüsse. XXXXX

Facebook	Referred the data subjects to their privacy policy and then stated other questions fell outside the scope of the GDPR.
Data Subject 1	**Response from controller:** Hello XXXXX, We refer to your request made pursuant to Articles 12 to 15 GDPR dated, XXX XXX. We respond as follows: Do you transmit data outside the EU? If so, to which countries? Please see the 'How do we operate and transfer data as part of our global services?' section of our Data Policy(https://www.facebook.com/policy.php)

	What legal basis is this transmission based on (e.g. decision on appropriateness, SCCs, BCRs, exceptions...)? Please see the 'How do we operate and transfer data as part of our global services? and the 'What is our legal basis for processing data?' sections of our Data Policy along with the legal basis information page, accessible from the 'Learn more' link in the 'What is our legal basis for processing data?' section of the Data Policy, which notes, among other things, that one of the core data uses necessary to provide our contractual services is to "[t]o transfer, transmit, store, or process your data outside the EEA, including to within the United States and other countries". If you have used SCCs or BCRs, please provide a copy of the SCCs or BCRs used for each transmission. Please see here: https://www.facebook.com/help/566994660333381?ref=dp When you transfer personal data to the US, does one of your partners fall under 50 USC 1881a (′′ FISA 702 ′′) or does it provide data to the US government according to EO 12.333? The information requested falls outside the scope of Articles 12 to 15 GDPR (and, for the avoidance of doubt, any other provision of the GDPR). If you send personal data to the US, what technical measures are you taking to prevent my personal data from being intercepted by the US government during the transmission? The information requested falls outside the scope of Articles 12 to 15 GDPR (and, for the avoidance of doubt, any other provision of the GDPR). However, we refer you to Appendix 2 in the Standard Contractual Clauses. If you transfer personal data to a US ′′ Electronic Communication Service Provider ′′ as defined in 18 U.S. Code 1881 (4) (b), or should you continue to follow the ′′ Privacy Shield ′′ during such transfers I ask you to stop the transmission of my personal data immediately. Please inform me within a week that you will stop the transmission or when you stop this transmission. This request falls outside the scope of Articles 12 to 15 GDPR (and, for the avoidance of doubt, any other provision of the GDPR). As explained in the 'How do we operate and transfer data as part of our global services?' section of our Data Policy, information controlled by Facebook Ireland Limited will be transferred or transmitted to, or stored and processed in, the United States or other countries outside of where you live for the purposes described in the Data Policy. These data transfers are necessary to provide the services set forth in the Facebook Terms of Service and to globally operate and provide these services. Facebook Ireland Limited
Data Subject 2	**Response from controller:** Sehr XXXXX Bitte beziehen Sie sich auf unsere Antwort, die Sie am XXXX XXX per Rückmeldung XXXXX erhalten haben. Mit freundlichen Grüßen Facebook Ireland Limited …… Sehr XXXXX,

	wir nehmen Bezug auf Ihre Anfrage gemäß den Artikeln 12 bis 15 DSGVO vom XXX XXXX. Wir antworten wie folgt: - Übermitteln Sie Daten außerhalb der EU? Wenn ja, in welche Länder? Informationen hierzu finden Sie im Abschnitt "Wie verarbeiten und übermitteln wir Daten im Rahmen unserer globalen Dienste?" in unserer Datenrichtlinie (https://www.facebook.com/policy.php). - Auf welche Rechtsgrundlage stützt sich diese Übermittlungen (z. B. Entscheidung über die Angemessenheit, SCCs, BCRs, Ausnahmen...)? Informationen hierzu finden Sie unter "Wie verarbeiten und übermitteln wir Daten im Rahmen unserer globalen Dienste?" und in dem Abschnitt "Was ist unsere Rechtsgrundlage für die Verarbeitung von Daten?" in unserer Datenrichtlinie (https://www.facebook.com/policy.php) sowie auf der Seite mit Informationen zu Rechtsgrundlagen, die über den Link "Erfahre mehr" im Abschnitt "Was ist unsere Rechtsgrundlage für die Verarbeitung von Daten?" unserer Datenrichtlinie (https://www.facebook.com/policy.php) erreichbar ist. Dort wird, unter anderem, darauf hingewiesen, dass eine der Hauptdatennutzungen, die zur Erbringung unserer vertraglichen Dienstleistungen erforderlich ist, darin besteht, Ihre Daten "in Länder außerhalb des EWR, einschließlich der USA und anderer Länder, zu übertragen und zu übermitteln bzw. dort zu speichern und zu verarbeiten". - Wenn Sie SCCs oder BCRs verwendet haben, legen Sie bitte für jede Übertragung eine Kopie der verwendeten SCCs oder BCRs vor. Ein Auszug der Standardvertragsklauseln, die Facebook Ireland Limited und Facebook, Inc. in Bezug auf die Übermittlung von Benutzerdaten aus der Region Europa (die „Standardvertragsklauseln") abgeschlossen haben, ist beigefügt. - Wenn Sie personenbezogene Daten in die USA übermitteln, fällt einer Ihrer Partner unter 50 USC §1881a ("FISA 702") oder stellt er der US-Regierung Daten gemäß EO 12.333 zur Verfügung? Die angeforderten Informationen fallen nicht in den Regelungsbereich der Artikel 12 bis 15 DSGVO (und, zur Klarstellung, auch nicht unter andere Bestimmungen der DSGVO). - Falls Sie personenbezogene Daten in die USA senden, welche technischen Maßnahmen ergreifen Sie, damit meine personenbezogenen Daten während der Übermittlung nicht von der US-Regierung abgefangen werden? Die angeforderten Informationen fallen nicht in den Regelungsbereich der Artikel 12 bis 15 DSGVO (und zur, Klarstellung, auch nicht unter andere Bestimmungen der DSGVO). Wir weisen jedoch auf Anhang 2 der Standardvertragsklauseln hin. - Wenn Sie personenbezogene Daten an einen US "Electronic Communication Service Provider" gemäß der Definition in 18 U.S. Code §1881(4)(b) übermitteln, oder sollten Sie sich bei solchen Übermittlungen weiterhin nach dem "Privacy Shield" vornehmen, bitte ich Sie, die Übermittlung meiner personenbezogenen Daten unverzüglich einzustellen. Bitte teilen Sie mir innerhalb einer Woche mit, dass Sie die Übertragung stoppen werden, bzw ab wann Sie dies Übermittlung stoppen. Ihre Anfrage fällt nicht in den Regelungsbereich der Artikel 12 bis 15 DSGVO (und zur, Klarstellung, auch nicht unter andere Bestimmungen der DSGVO). Wie im Abschnitt „Wie verarbeiten und übermitteln wir Daten im Rahmen unserer globalen Dienste?" in unserer Datenrichtlinie (https://www.facebook.com/policy.php) erläutert, werden von Facebook Ireland Limited kontrollierte Informationen in die USA oder in andere Länder außerhalb des Landes, in dem Sie leben, für die in der Datenrichtlinie (https://www.facebook.com/policy.php) beschriebenen Zwecke, übertragen oder dort gespeichert und verarbeitet. Diese Datenübertragungen sind erforderlich, um die in den Facebook-Nutzungsbedingungen festgelegten Dienste zu erbringen und diese Dienste weltweit zu betreiben und zu erbringen. Wenn Sie nicht möchten, dass Ihre persönlichen Daten im Rahmen der Bereitstellung und des Betriebs des Facebook-Dienstes übertragen werden, können Sie Ihr Konto jederzeit löschen, indem Sie die Schritte befolgen, die unter "Wie kann ich mein

	Facebook-Konto dauerhaft löschen?" aufgeführt sind: https://www.facebook.com/help/224562897555674. Mit freundlichen Grüßen, Facebook Ireland Limited

GMX	Referred data subject to their different website policies.
Data Subject 1	**Response from controller:** Sehr XXXXX, vielen Dank für Ihre Anfrage. Wir würden Sie gerne darum bitten, die gestellte Auskunftsanfrage zu präzisieren, denn in der jetzigen Form ist es uns nicht erlaubt, darauf zu antworten und damit unserer rechtlichen Verpflichtung nachzukommen, denn Artikel 12, 13, 14 und 15 der DSGVO haben einen unterschiedlichen Inhalt und stimmen nicht mit den Fragen, die Sie stellen überein. Deswegen brauchen wir eine Klarstellung, damit wir verstehen können, ob Sie sich nur auf bestimmte Informationen beziehen oder auf alle möglichen Informationen (was es wiederum unmöglich macht diese konkret zu beantworten). Was wir tun können ist, die spezifischen Fragen zu beantworten, die Sie uns gestellt haben: Im Bezug auf Ihre erste Frage sollten Sie zuerst klären, ob Sie sich hierzu auf die Übermittlung Ihrer persönlichen Daten an Drittstaaten beziehen, da die Übermittlung von Daten außerhalb der EU an sich nicht datenschutzrelevant ist. In der Zwischenzeit verweisen wir Sie auf den Inhalt unserer Datenschutzerklärung, in der die Übermittlung personenbezogener Daten für jeden unserer Dienste und Produkte ausdrücklich erwähnt wird. (https://agb-server.gmx.net/datenschutz-at/). Was die zweite Frage betrifft, so benötigen wir hier auch eine Klärung, da wir nicht sicher sind, auf welche Verarbeitung Sie sich beziehen. Auch hier gilt, dass die verschiedenen Rechtsgrundlagen für jede unserer Datenverarbeitungen (und darunter natürlich auch diejenigen, die eine Übermittlung an Dritte im Sinne des Datenschutzes erfordern) in unserer Datenschutzerklärung stets aktualisiert werden. (https://agb-server.gmx.net/datenschutz-at/). Im Zusammenhang mit Ihrer zweiten Frage können wir Ihnen die Vertragsunterlagen, die uns an unsere Partner binden, nicht zur Verfügung stellen. Was wir tun können, ist, Sie auf der Grundlage von Artikel 15 Absatz 2 DSGVO über die Maßnahmen im Zusammenhang mit Artikel 46 DSGVO zu informieren. Wir bitten Sie, zu bestätigen, ob dies der Zweck Ihrer Frage ist. In jedem Fall finden Sie weitere Informationen in unserer Datenschutzerklärung. (https://agb-server.gmx.net/datenschutz-at/) Was Ihre dritte Frage betrifft, so können wir weder Informationen über Drittfirmen beantworten noch die rechtliche Situation dieser Firmen analysieren. Im Prinzip ist jedes Unternehmen in den USA föderalen Vorschriften untergeordnet, ob es anwendbar ist oder nicht, hängt von jedem spezifischen Fall ab, und wir können und dürfen keine generische Antwort geben. Eine Liste der Sicherheitsmaßnahmen, die wir bei unserer Arbeit mit Drittfirmen (die nicht unbedingt Dritte im Sinne des Datenschutzes sein müssen) als Standard anwenden, finden Sie unter folgendem Link: (https://agb-server.gmx.net/gmxagb-at/#Annex%20-%20Technische%20und%20organisatorische%20Ma%C3%9Fnahmen%20des%20Auftragnehmers). In jedem Fall werden, abhängig von der Art der Verarbeitung, diese Maßnahmen gesteigert. Auch dies ist ein Fall, der nicht allgemein beantwortet werden kann.

	Wenn Sie es für angebracht halten und Ihre Fragen präzisieren möchten, helfen wir Ihnen gerne weiter. Sollte die Antwort nicht zu Ihrer Zufriedenheit ausgefallen sein, teilen wir Ihnen mit, dass Sie Ihr Beschwerderecht bei der folgenden Aufsichtsbehörde geltend machen können: Österreichische Datenschutzbehörde Wickenburggasse 8 1080 Wien Mit freundlichen Grüßen

Google	Claim that they will transition over to Standard Contractual Clauses.
Data subject 1	**Response from controller:** Liebe Google Nutzerin, lieber Google Nutzer, hiermit dürfen wir Ihnen den Eingang Ihrer Anfrage bezüglich des EU-U.S. Privacy-Shield Abkommens bestätigen. Wir hoffen, dass die nachfolgenden Informationen hilfreich für Sie sind und Ihre Anfrage beantworten. Google bietet ein umfassendes Programm zur Einhaltung der Privacy-Shield-Richtlinien an, das eine eingehende Bewertung der Google Produkte beinhaltet, um sicherzustellen, dass jedes Produkt den Prinzipien des Privacy-Shields entspricht. Sowohl das EU-U.S. Privacy-Shield als auch das Siss-U.S. Privacy-Shield wurden seit 2016 bis zum jüngsten Urteil des Europäischen Gerichtshofs (EuGH) als ein angemessenes Schutzniveau für personenbezogene Daten nach europäischem Datenschutzrecht angesehen. Diese Zertifizierung wurde jedes Jahr erneuert. Google wurde zuletzt im September 2019 rezertifiziert. Wir haben die Entwicklungen im Zusammenhang mit internationalen Datentransfers, die nach der DSGVO zulässig sind, konstant mitverfolgt und sind uns der Forderung nach einer Grundlage für Datentransfers in Übereinstimmung mit der DSGVO bewusst. Vor dem Hintergrund des jüngsten EuGH-Urteils werden wir dazu übergehen, bei Datentransfers von personenbezogenen Daten aus dem Europäischen Wirtschaftsraum und dem Vereinigten Königreich sowie der Schweiz auf Standardvertragsklauseln zurückzugreifen, die gemäß dem Urteil weiterhin einen gültigen Rechtsrahmen für den Datentransfer im Rahmen der DSGVO bilden. Je nach Produkt wurden unsere Kunden und Nutzer über diese Änderungen bereits informiert bzw. werden eine solche Information erhalten, sobald Standardvertragsklauseln zur Verfügung stehen. Mit freundlichen Grüßen Ihr Google Team

Hinge	No further response from controller so far.
Data subject 1	**Response from controller:** Hi there, We have received your inquiry and will reach out soon. In the meantime, if there is anything else we may do for you please do not hesitate to reach out. Sincerely,

Hotels.com	Currently evaluating the situation.
Data subject 1	**Response from controller:** Sehr XXXXX Vielen Dank für Ihre kürzliche E-Mail. Wir verstehen Ihre Fragen im Zusammenhang mit dem EuGH-Urteil in Schrems II. Wie die meisten internationalen Unternehmen prüfen wir derzeit die Auswirkungen dieser Entscheidung, um festzustellen, welche Maßnahmen wir gegebenenfalls ergreifen müssen, um unsere bestehenden Compliance-Praktiken zu ergänzen. Wir sind daher derzeit nicht in der Lage, auf bestimmte Fragen bezüglich des Urteils zu antworten, können Sie jedoch gerne bei der Ausübung Ihrer datenschutzrechtlichen Rechte auf Zugang, Berichtigung, Widerspruch und Löschung gemäß der DSGVO unterstützen. Bitte teilen Sie uns mit, ob Sie eines dieser Rechte ausüben möchten. Mit freundlichen Grüßen

Instagram	Referred the data subjects to their privacy policy and then stated other questions fell outside the scope of the GDPR.
Data subject 1	**Response from controller:** Dear XXXXX; We refer to your request made pursuant to Articles 12 to 15 GDPR dated, XXX XXX. We respond as follows: Do you transmit data outside the EU? If so, to which countries? Please see the 'How do we operate and transfer data as part of our global services?' section of our Data Policy(https://www.facebook.com/policy.php) What legal basis is this transmission based on (e.g. decision on appropriateness, SCCs, BCRs, exceptions...)? Please see the 'How do we operate and transfer data as part of our global services? and the 'What is our legal basis for processing data?' sections of our Data Policy along with the legal basis information page, accessible from the 'Learn more' link in the 'What is our legal basis for processing data?' section of the Data Policy, which notes, among other things, that one of the core data uses necessary to provide our contractual services is to "[t]o transfer, transmit, store, or process your data outside the EEA, including to within the United States and other countries".

	If you have used SCCs or BCRs, please provide a copy of the SCCs or BCRs used for each transmission. Please see here: https://www.facebook.com/help/566994660333381?ref=dp When you transfer personal data to the US, does one of your partners fall under 50 USC 1881a (" FISA 702 ") or does it provide data to the US government according to EO 12.333? The information requested falls outside the scope of Articles 12 to 15 GDPR (and, for the avoidance of doubt, any other provision of the GDPR). If you send personal data to the US, what technical measures are you taking to prevent my personal data from being intercepted by the US government during the transmission? The information requested falls outside the scope of Articles 12 to 15 GDPR (and, for the avoidance of doubt, any other provision of the GDPR). However, we refer you to Appendix 2 in the Standard Contractual Clauses. If you transfer personal data to a US " Electronic Communication Service Provider " as defined in 18 U.S. Code 1881 (4) (b), or should you continue to follow the " Privacy Shield " during such transfers I ask you to stop the transmission of my personal data immediately. Please inform me within a week that you will stop the transmission or when you stop this transmission. This request falls outside the scope of Articles 12 to 15 GDPR (and, for the avoidance of doubt, any other provision of the GDPR). As explained in the 'How do we operate and transfer data as part of our global services?' section of our Data Policy, information controlled by Facebook Ireland Limited will be transferred or transmitted to, or stored and processed in, the United States or other countries outside of where you live for the purposes described in the Data Policy. These data transfers are necessary to provide the services set forth in the Facebook Terms of Service and to globally operate and provide these services.

LinkedIn	Claim that they rely on Standard Contractual Clauses to some data subjects, and didn't respond fully to others.
Data subject 1	**First response from controller:** Hi XXXXX, I'm sorry for not having a quick answer about your issue. I've forwarded your message to another group for additional review and advice. We'll be in contact with you as quickly as possible, but your issue may require additional research, which may extend your wait time. We ask that you don't create any additional cases in the meantime and thank you in advance for your patience. LinkedIn Trust & Safety --- **Second response from controller:** Hello XXXXX, Thank you for getting in touch, and sincere apologies for the delay.

	We're aware of the Schrems II ruling by the ECJ and want to be clear that as a customer of LinkedIn, the ruling does not change your ability to continue using our products. For years we have relied on overlapping protections under both Standard Contractual Clauses (SCCs) and the Privacy Shield legal frameworks for data transfers. While this ruling invalidated the use of Privacy Shield, the SCCs remain in place. As you are already protected under the SCCs, your ability to use our products remains unchanged. Although you did not request a copy of your data, please see this for information purposes: https://www.linkedin.com/help/linkedin/answer/50191/accessing-your-account-data?lang=en If you have any further questions, please let us know. Regards,
Data subject 2	**Response from controller:** Hi XXXXX, I'm sorry for not having a quick answer about your issue. I've forwarded your message to another group for additional review and advice. We'll be in contact with you as quickly as possible, but your issue may require additional research, which may extend your wait time. If you can log into your account, you can always check the status of your case on LinkedIn: 1. Click the Me icon (your profile photo) at the top of your LinkedIn homepage. 2. Select Open Quick Help from the dropdown and click Go to Help Homepage. 3. On the Help page, click your profile photo in the top right, and then select View your cases from the dropdown to see the status of any cases you've submitted. Please note that if you aren't able to login for any reason, you won't be able to check the status of your case. We ask that you don't create any additional cases in the meantime. We're working as quickly as possible to resolve your inquiry. Thanks for your patience. Regards,
Data subject 3	**First response from controller:** Hi XXXXX, I'm sorry for not having a quick answer about your issue. I've forwarded your message to another group for additional review and advice. We'll be in contact with you as quickly as possible, but your issue may require additional research, which may extend your wait time. We ask that you don't create any additional cases in the meantime and thank you in advance for your patience. LinkedIn Trust & Safety --- **Second response from controller:**

	Hello XXXXX, Thank you for getting in touch, and sincere apologies for the delay. We're aware of the Schrems II ruling by the ECJ and want to be clear that as a customer of LinkedIn, the ruling does not change your ability to continue using our products. For years we have relied on overlapping protections under both Standard Contractual Clauses (SCCs) and the Privacy Shield legal frameworks for data transfers. While this ruling invalidated the use of Privacy Shield, the SCCs remain in place. As you are already protected under the SCCs, your ability to use our products remains unchanged. Although you did not request a copy of your data, please see this for information purposes: https://www.linkedin.com/help/linkedin/answer/50191/accessing-your-account-data?lang=en If you have any further questions, please let us know. Regards, LinkedIn Privacy and Intellectual Property Escalations

Mango	Claim that they rely on Standard Contractual Clauses.
Data subject 1	**Response from controller:** Hallo XXXXX, wir kontaktieren Sie bezüglich Ihrer Anfrage auf Datenschutzrecht. Wir möchten Sie darüber informieren, dass wir in Ihrem Fall Ihre persönlichen Daten, konkret Ihre E-Mail-Adresse, an SALESFORCE.com Emea Limited übertragen haben. Das Unternehmen erbringt uns Dienstleistungen als Datenverarbeiter und ist in den USA ansässig. Um einen angemessenen Schutzniveau Ihrer Daten bei Übertragung an Länder außerhalb des Europäischen Wirtschaftsraums zu gewährleisten, setzt MANGO die entsprechenden Maßnahmen um, wie die von der Aufsichtsbehörde angewendeten und von der Europäischen Kommission verabschiedeten Datenschutz-Standardklauseln (Art. 46 der Datenschutz-Grundverordnung, DSGVO). Über dem folgenden Link der spanischen Agentur für Datenschutz (AEPD) können Sie auf die Standardklauseln zugreifen: https://www.aepd.es/sites/default/files/2019-09/2010D0087-es%20%281%29.pdf Die Übertragung personenbezogener Daten erfolgt verschlüsselt unter Verwendung eines kryptografischen Protokolls, wodurch der Datenaustausch in einer sicheren und privaten Umgebung zwischen dem Datenverantwortlichen und dem Datenverarbeiter vorgenommen wird (TLS 1.2). Es ist hinzuzufügen, dass SALESFORCE.com Emea Limited nicht auf der Liste der Unternehmen steht, die Daten über US-Überwachungsprogramme wie PRISM oder UPSTREAM gemäß Artikel 702 des FISA (Foreign Intelligence Surveillance Act) mit der US-Regierung teilen. Wir informieren Sie, dass Sie das Recht haben, den Rest der in den Art. 15-22 der Datenschutz-

	Grundverordnung 2016/679 anerkannten Rechte auszuüben und gegebenenfalls jegliche Einsprüche bei der zuständigen Kontrollbehörde einzureichen. Mit freundlichen Grüßen,

Mastercard	Claim that they rely on Binding Corporate Rules.
Data subject 1	**Response from controller:** Dear XXXXX Thank you for contacting Mastercard. I understand that you are interested in Mastercard's privacy and data protection practices, in particular how Mastercard complies with the European Union ("EU")'s rules regarding the crossborder transfer of personal data. Privacy and data protection are at the core of our business and embedded into the design of all our products and services. We value the questions received from individuals regarding our privacy and data protection practices and do our utmost to provide them with fair and transparent information. Mastercard is aware of the recent European Court of Justice decision affecting transfers of EU personal data to the United States ("U.S.") and is carefully assessing its impact on individuals and on our business. We are closely monitoring the guidance from the European Data Protection Board and the Belgian Data Protection Authority (Mastercard's lead data protection authority), specifically in relation to what would constitute supplemental safeguards for data transfers outside of the EU. Information about cross-border data transfers at Mastercard Mastercard is a global business and may transfer your personal data to the United States and other countries. In particular, we transfer payment card transaction data for the purpose of payment processing to our secure databases located in the U.S and to other locations when you pay with your Mastercard payment card anywhere around the world. Mastercard has implemented a set of Binding Corporate Rules which have been recognized by EU data protection authorities as providing appropriate safeguards to the processing of personal data by Mastercard globally. Our Binding Corporate Rules have been approved by EU data protection authorities in late 2016, and are available at: https://www.mastercard.com/content/dam/mccom/global/documents/mastercard-bcrs.pdf. To the best of our knowledge, we do not share transaction data we process for payment processing with partners that are "electronic communication service providers" as defined in 18 U.S. Code §1881(4)(b), and all transaction data processed by Mastercard is encrypted in transit. We do not rely on the EU-US Privacy Shield for payment processing. Information or actions regarding your personal data I understand that you are a Mastercard cardholder and that you would like Mastercard to consider taking certain actions with regard to personal data that Mastercard may process about you. When you use a Mastercard payment card to buy a good or service, Mastercard only receives limited types of data and processes that data as a data processor on behalf of your financial institution. This data typically does not include your name or address, and is limited to transaction details such as the card account number(s), date, time and amount of the transaction, and name and location of the merchant. Your financial institution is the data controller for the processing of your transaction data and is, therefore, the entity legally responsible for handling your request. Thus, if you would like to

	exercise your rights under the EU General Data Protection Regulation with respect to such data, please contact your financial institution. In limited situations, we act as a data controller, for example we offer cardholders certain loyalty and marketing programs such as Priceless Cities. If you would like us to assess whether we process and transfer your personal data as a data controller, we will need to authenticate you. In that case, please provide us with a copy of your ID document or passport and your Mastercard payment card number in a secure manner. We suggest that you redact the copy of your ID except for the following data: surname, first name and date of birth. The copy of your ID or passport will be immediately deleted once we have verified your identity. For more information about Mastercard's privacy practices, including cross-border data transfers, please see our Global Privacy Notice available at: https://www.mastercard.co.uk/en-gb/aboutmastercard/what-we-do/privacy.html. I hope that I have been able to address your concerns. If you are not satisfied you have the possibility of lodging a complaint with an EU data protection authority and seeking a judicial remedy. Should you have any further questions, please do not hesitate to contact me. Sincerely,
Data Subject 2	**First response from controller:** Dear Sir, Madam, Thank you for contacting Mastercard. Mastercard respects your privacy and will address your request promptly. In order for us to process your request, we need to understand where you are located. Please reply to this email indicating the country where you are located so that we can direct your request appropriately. Sincerely, Mastercard --- **Second response from controller:** Dear XXXXX, Thank you for contacting Mastercard. I understand that you are interested in Mastercard's privacy and data protection practices, in particular how Mastercard complies with the European Union ("EU")'s rules regarding the crossborder transfer of personal data. Privacy and data protection are at the core of our business and embedded into the design of all our products and services. We value the questions received from individuals regarding our privacy and data protection practices and do our utmost to provide them with fair and transparent information.

	Mastercard is aware of the recent European Court of Justice decision affecting transfers of EU personal data to the United States ("U.S.") and is carefully assessing its impact on individuals and on our business. We are closely monitoring the guidance from the European Data Protection Board and the Belgian Data Protection Authority (Mastercard's lead data protection authority), specifically in relation to what would constitute supplemental safeguards for data transfers outside of the EU. Information about cross-border data transfers at Mastercard Mastercard is a global business and may transfer your personal data to the United States and other countries. In particular, we transfer payment card transaction data for the purpose of payment processing to our secure databases located in the U.S and to other locations when you pay with your Mastercard payment card anywhere around the world. Mastercard has implemented a set of Binding Corporate Rules which have been recognized by EU data protection authorities as providing appropriate safeguards to the processing of personal data by Mastercard globally. Our Binding Corporate Rules have been approved by EU data protection authorities in late 2016, and are available at: https://www.mastercard.com/content/dam/mccom/global/documents/mastercard-bcrs.pdf. To the best of our knowledge, we do not share transaction data we process for payment processing with partners that are "electronic communication service providers" as defined in 18 U.S. Code §1881(4)(b), and all transaction data processed by Mastercard is encrypted in transit. We do not rely on the EU-US Privacy Shield for payment processing. Information or actions regarding your personal data When you use a Mastercard payment card to buy a good or service, Mastercard only receives limited types of data and processes that data as a data processor on behalf of your financial institution. This data typically does not include your name or address, and is limited to transaction details such as the card account number(s), date, time and amount of the transaction, and name and location of the merchant. Your financial institution is the data controller for the processing of your transaction data and is, therefore, the entity legally responsible for handling your request. Thus, if you would like to exercise your rights under the EU General Data Protection Regulation with respect to such data, please contact your financial institution. In limited situations, we act as a data controller, for example we offer cardholders certain loyalty and marketing programs such as Priceless Cities. If you would like us to assess whether we process and transfer your personal data as a data controller, we will need to authenticate you. In that case, please provide us with a copy of your ID document or passport and your Mastercard payment card number in a secure manner. We suggest that you redact the copy of your ID except for the following data: surname, first name and date of birth. The copy of your ID or passport will be immediately deleted once we have verified your identity. For more information about Mastercard's privacy practices, including cross-border data transfers, please see our Global Privacy Notice available at: https://www.mastercard.co.uk/en-gb/aboutmastercard/what-we-do/privacy.html.

	I hope that I have been able to address your concerns. If you are not satisfied you have the possibility of lodging a complaint with an EU data protection authority and seeking a judicial remedy. Should you have any further questions, please do not hesitate to contact me. Sincerely

Microsoft	Claim they rely on Standard Contractual Clauses.
Data Subject 1	**Response from controller:** Sehr XXXXX vielen Dank, dass sie Microsoft kontaktiert haben. Wir nehmen den Schutz der Privatsphäre und die Sicherheit unserer Kunden und ihrer Daten ernst und beantworten gerne alle Ihre Fragen, die im Folgenden nacheinander gestellt werden. • Übermitteln Sie Daten außerhalb der EU? Wenn ja, an welche Länder? Microsoft bietet eine breite Produktpalette an und je nach Dienstleistung können wir Daten an Länder außerhalb der EU übermitteln. Unsere Datenschutzerklärung erläutert, wie und wo Microsoft personenbezogene Daten verarbeiten kann, um unsere Dienstleistungen zu erbringen. Diesbezüglich verweisen wir Sie auf die folgende Bestimmung unserer Datenschutzerklärung https://privacy.microsoft.com/de-de/privacystatement: Die von Microsoft gesammelten personenbezogenen Daten können in Ihrer Region, in den USA und in jedem anderen Land gespeichert und verarbeitet werden, in dem Microsoft oder seine verbundenen Unternehmen, Tochtergesellschaften oder Dienstanbieter Einrichtungen unterhalten. Microsoft verwaltet große Rechenzentren in Australien, Österreich, Brasilien, Kanada, Chile, Finnland, Frankreich, Deutschland, Hong Kong, Indien, Irland, Japan, Korea, Luxemburg, Malaysia, den Niederlanden, Singapur, Südafrika, dem Vereinigten Königreich und den USA. In der Regel befindet sich der primäre Speicherort in der Region des Kunden oder in den Vereinigten Staaten, mit einer Datensicherung in einem Rechenzentrum in einer anderen Region. Die Speicherorte werden effizient, zur Verbesserung der Leistung und zum Erstellen von Redundanzen ausgewählt, um die Daten im Falle eines Stromausfalls oder bei einem anderen Problem zu schützen. Wir unternehmen Schritte, um sicherzustellen, dass die Daten, die wir im Rahmen dieser Datenschutzbestimmungen sammeln, den Bestimmungen dieser Erklärung und den Anforderungen an das geltende Recht entsprechen wo immer sich diese Daten auch befinden. • Was ist die Rechtsgrundlage für diese Übermittlungen (z.B. Angemessenheitsbeschluss, Standardvertragsklauseln (SCCs), verbindliche interne Datenschutzvorschriften (BCRs), Ausnahmen..?) Microsoft hat über lange Zeit zwei Mechanismen eingesetzt, um die rechtmäßige Übermittlung von Daten aus Europa in die USA sicherzustellen – Standardvertragsklauseln (SCCs) und den EU-U.S.-Privacy Shield. Nachdem das Privacy Shield kürzlich für ungültig erklärt wurde, wird sich Microsoft weiterhin auf die SCCs als Rechtsgrundlage für die Übermittlungen stützen.

	• Wenn Sie Standardvertragsklauseln (SCCs) oder verbindliche interne Datenschutzvorschriften (BCRs) verwendet haben, legen Sie bitte für jede Übermittlung eine Kopie der verwendeten SCCs oder BCRs vor. Wir haben eine PDF-Datei mit den SCCs beigefügt, die wir als Rechtsgrundlage für die Übermittlungen verwenden. • Wenn Sie personenbezogene Daten in die USA übermitteln, fällt einer Ihrer Partner unter USC 1881a ("FISA 702") oder stellt er der US-Regierung Daten gemäß EO 12.333 zur Verfügung? Microsoft hat unseren Transparenzbericht über Auskunftsverlangen der U.S.-Regierung an folgender Stelle veröffentlicht: https://www.microsoft.com/corporate-responsibility/us-national-security-orders-report. • Wenn Sie personenbezogene Daten in die USA übermitteln, welche technischen Maßnahmen ergreifen Sie, um zu verhindern, dass meine personenbezogenen Daten während der Übermittlung von der US-Regierung abgefangen werden? Wir fühlen uns dem Schutz der Privatsphäre und der Sicherheit unserer Kunden und ihrer Daten zutiefst verpflichtet. Seit vielen Jahren trifft Microsoft zusätzliche technische Schutzvorkehrungen, einschließlich der Verschlüsselung, die über den Schutz hinausgehen, zu dem wir uns in den Standardvertragsklauseln verpflichten. Weitere Einzelheiten zur Verschlüsselung als zusätzliche Schutzvorkehrung finden Sie in der folgenden Beschreibung unserer Verschlüsselungspraktiken. Microsoft verwendet Verschlüsselung nach Industriestandard, um Daten während der Übertragung und wenn sie gespeichert sind zu schützen. Unsere Produkte sind auf Betriebssicherheit ausgelegt und orientieren sich an bewährten Verfahren für Softwaresicherheit. Unser Security Development Lifecycle (SDL) berücksichtigt Sicherheits- und Datenschutzaspekte in allen Phasen des Entwicklungsprozesses und unterstützt Entwickler bei der Erstellung hochsicherer Software, der Einhaltung von Sicherheitsanforderungen und der Reduzierung von Entwicklungskosten. Unsere wichtigsten Dienste verwenden Transport Layer Security (TLS) zum Schutz der Kommunikation, sei es von einem Client zu einem anderen Client, wie z. B. ein Skype-Anruf oder Client-Verbindungen zu Microsoft, z. B. wenn ein Dokument auf Office OneDrive hochgeladen wird. Darüber hinaus werden Daten, die zur Unterstützung der Verwendung unserer Produkte verwendet werden, z. B. Windows-Diagnosedaten, verschlüsselt, wenn sie entweder vom Client-Gerät oder bei der Weiterleitung zu und von Rechenzentren aufgrund von Kapazitäts- oder Lastanforderungen übertragen werden. Gespeicherte Daten werden bei vielen unserer Hauptprodukte nach dem AES-256 Standard verschlüsselt, einschließlich bei Office und Bing, die auch die umfangreichen Verschlüsselungsmöglichkeiten für auf der Azure Plattform gespeicherte Daten nutzen, um Kundendaten zu sichern: • Azure Disk Encryption (BitLocker): https://docs.microsoft.com/azure/virtual-machines/windows/disk-encryption • Azure Storage: https://docs.microsoft.com/azure/storage/common/storage-service-encryption • Azure SQL: https://docs.microsoft.com/azure/azure-sql/database/transparent-data-encryption-tde-overview?tabs=azure-portal • Azure Cosmos DB: https://docs.microsoft.com/azure/cosmos-db/database-encryption-at-rest Als Beispiel für den Ende-zu-Ende-Ansatz von Microsoft zum Schutz der Benutzerinformationen implementiert die Suchmaschine Bing von Microsoft die Transport Layer Security (TLS) zur Sicherung der Suchvorgänge und Interaktionen eines Kunden. Sobald sich die Daten aus den Suchvorgängen von Bing in den Rechenzentren von Microsoft befinden, verschlüsseln und sichern unsere Dienste weiterhin Inhalte wie die von Ihnen eingegebenen Suchvorgänge, die Diagnoseinformationen, die wir

	über die Interaktionen eines Kunden (wie Seitenaufrufe oder Klicks) erfassen, und die erforderlichen Informationen, die Bing verwendet, um die Plattform vor betrügerischen Aktivitäten und externen Angriffen zu schützen und zu sichern. Microsoft sichert die Suchhistorie eines Kunden mit branchenüblichen Verschlüsselungsroutinen (FIPS 140-2 Standard kompatible Verschlüsselung, z.B. AES-256). Inter-Datacenter Übermittlungen werden mit den ähnlichen TLS-Protokollen gesichert, und Daten werden im Ruhezustand mit branchenführenden Technologien geschützt, wie BitLocker Drive Encryption, Transparent Data Encryption (für Azure SQL), und proprietären Systemen. • Wenn Sie einem Anbieter von elektronischen Kommunikationsdiensten gemäß der Definition in 18 U.S. Code s.1881(4)(b) personenbezogene Informationen zur Verfügung stellen oder wenn Sie solche Übermittlungen weiterhin auf das Privacy Shield stützen, bitte ich Sie, die Übermittlung meiner personenbezogenen Daten sofort zu unterlassen. Teilen Sie mir bitte innerhalb einer Woche mit, dass Sie die Übermittlung stoppen werden oder wann sie die Übermittlung stoppen werden. Wir haben Ihr Ersuchen zur Kenntnis genommen und prüfen es derzeit. Wir hoffen, dass die obigen Informationen hilfreich sind. Bitte lassen Sie mich wissen, wenn Sie weitere Fragen haben. Mit freundlichen Grüßen, Microsoft-Datenschutz-Abteilung

Netflix	No substantial response from Netflix.
Data Subject 1	**Response from controller:** Thank you for your inquiry. Your email has reached an automated mailbox, which is reviewed regularly and is intended only for inquiries and requests regarding our privacy practices, as set forth in our Privacy Statement at https://www.netflix.com/privacy. Answers to the most common privacy questions we receive can be found here. We do not respond to general customer service or other types of inquiries through this email address. For non-privacy related questions, please refer to our Help Center, or contact our Customer Service department via chat or phone, through https://help.netflix.com. Information regarding our company can also be found at our Media Center (https://media.netflix.com) and through the other links in the footer of our main site (www.netflix.com). Sincerely, Netflix

Nike	Claim that they rely on Standard Contractual Clauses.
Data Subject 1	**Response from controller:** Dear XXXXX, In response to your request dated XXX XXX, we wanted to provide you with additional information on how Nike handles personal data. We collect personal data to provide you with the products or services you request. For example, if you make a purchase on Nike.com or participate in a Nike event or promotion, we will use the contact information you provide us to communicate with you about the purchase, event or promotion.

	We retain personal data for as long as is necessary to carry out the purpose for which it was given (unless a longer retention period is required by law). Inactive Nike account holders and other users will be deactivated and eventually have their personal data deleted in line with Nike's data retention policy. Click here to learn more. We may also collect personal data from you to enable particular features within our websites and apps. For example, we request your physical location to log your run route when you use our Nike Run Club (NRC) app. Nike does not sell consumer details to third parties. Nike does however, like most companies, work in collaboration with service providers (data processors) who process the data on our behalf, for specific purposes. For example, to process credit cards and payments, shipping and deliveries, host, manage and service our data, distribute emails, conduct research and analysis to improve our products and services, manage brand and product promotions as well as administer certain services and features. We will always take steps to ensure your personal data is protected in these circumstances and we always take measures to comply with legal requirements for the international transfer of personal data. The personal data we collect (or process) in the context of our Sites and Apps will be stored in the USA and other countries. Some of the data recipients with whom Nike shares your personal data may be located in countries other than the country in which your personal data originally was collected. The laws in those countries may not provide the same level of data protection compared to the country in which you initially provided your data. Nevertheless, when we transfer your personal data to recipients in other countries, including the USA, we will protect that personal data as described in this privacy policy and in compliance with applicable law. We take measures to comply with applicable legal requirements for the transfer of personal data to recipients in countries outside of the EEA or Switzerland that do not provide an adequate level of data protection. We use a variety of measures to ensure that your personal data transferred to these countries receives adequate protection in accordance with data protection rules, including signing the EU Standard Contractual Clauses. Where personal data is transferred within Nike, we use an intragroup data transfer agreement. If you have any questions or would like to file a privacy complaint or request more information on Nike's privacy commitments, please contact the Nike Privacy Office at privacy@nike.com. Nike values your privacy and is committed to protecting the personal data of all of its consumers.

OneTrust	Did not specify what transfer mechanism they rely on.
Data Subject 1	**Response from controller:** Hello XXXXX, As many of you know by now, the CJEU invalidated the EU-US Privacy Shield and added uncertainty around the ability to use Standard Contract Clauses (SCC) for data transfers to the US. We understand customers are eager to hear from us on our plan to support your OneTrust cloud deployment in this new environment. OneTrust is dedicated to taking a leading position here, and I am proud of the internal OneTrust privacy and security team for proactively monitoring these developments via our OneTrust DataGuidance solution, and preparing for any possible outcome ahead of time.

I am pleased to say that OneTrust will be providing multiple solutions for customers to select from if you are impacted by this ruling. Customers will be able to choose based on which offering that they determine best fits their unique business situation and interpretation of how the decision impacts SCCs. These are:

- Opting-in to an enhanced EU hosting to be fully containerized in EU
- Continuing to rely on SCC, and migrating to a future enhanced SCC if/when as they become available
- Full on-premise or private cloud hosting

Our customers can learn more about these options and steps you can take in our myOneTrust portal.

OneTrust customers already have the option to choose from 10 data center locations in Germany, France, Australia, Brazil, Canada, India, Singapore, Switzerland, the United Kingdom and the United States.

As the first company in the world to achieve ISO 27701, our demonstrated track record of building technology based on strict standards is core to our mission. In collaboration with our Customer Advisory Board (CAB), OneTrust is dedicated to maintaining a high level of controls to support our customers and honour the Schrems II decision.

We will continue to provide OneTrust customers with updates, analysis and guidance on the myOneTrust portal. Additionally, we have made free resources available as you look to understand the impact of this decision on your business and work toward a new form of compliance. These resources will be continuously updated and include:

- Post-Decision and analysis webinar, led by an expert panel
- Future webinars on what the Schrems II decision means for your privacy program
- In-depth articles and analysis about the Schrems II decision
- The Data Transfer Comparison Tool updated with Schrems II guidance to help professionals review and compare regulations across multiple jurisdictions at a glance

You can contact us today to learn about our EU containerized solution as well as other OneTrust products to help your business adjust for the Schrems II ruling, and as always, I am personally at your service.

Thank you,

Reply from data subject:

Dear XXXXX,

I am sure one OneTrust is protecting my data as well.

	therefore, could you please indicate where you obtained my data (since I am not a customer), on which basis your are processing to do marketing via email, and also provide me with all the information as per article 15 GDPR. Should you not answer within one month, I will of course file a complaint with my DPA. Best XXXXX --- **Response from controller:** XXXXX, Thank you for your request. We are happy to assist you with it. Your message brought to our attention that the event web form was designed for a more narrow audience and yet was applied more broadly during a rush to make website changes. We are taking steps to review and correct this and ensure it works for a global audience. In response to your request for information according to Article 15, please find attached the specific data elements that we process about you and the following information about the processing: What information does OneTrust collect about you and why? We collect information that you provide to us directly, including contact information, such as first name, last name, e-mail address, job title and company name, as well as other information that could be on your business card (such as your company address and phone number) when you visit our website or talk to us at a conference or other event, or if you are a customer. We use the information you provide to deliver our products and services, to send you some privacy and/or security content that we make available on our website and that you requested, or to get in touch with you about a demo/trial. We also use it to support our marketing efforts, including contacting you to provide additional information on our products and services. For customers, we use it to set up your customer account. We also collect some information automatically: when you visit our website (such as your device's IP address, what pages your device visited) or when you use our services (usage information, log information and information collected by cookies and other similar technologies). We use information we collect automatically to administer our website and enhance your visitor experience, for our marketing efforts to serve ads across websites, and for security purposes. Read our full privacy notice. What are the categories? Please find the categories of personal data that we process about you listed below: Basic Information (e.g., name, company, title, email) Consent Details Address Details Past Activity

	**Some personal data may have been redacted, i.e. to protect the rights and freedoms of other individuals whose personal data may have appeared in conjunction with yours. How do we use the information about you? Websites or Events: We will use the information we collect via our Websites: To administer our Website, our events and for internal operations, including troubleshooting, data analysis, testing, statistical and survey purposes; To improve our Website to ensure that content is presented in the most effective manner for you and for your computer; For trend monitoring, marketing and advertising; For purposes made clear to you at the time you submit your information – for example, to fulfill your request for a demo, to provide you with access to one of our webinar's or whitepaper's or to provide you with information you have requested about our Services; and As part of our efforts to keep our Website secure. How long do we hold on to the data about you? With respect to processing of your personal data, we hold on to the data only for as long as it is still necessary to fulfill the purpose for which it was originally collected. With respect to marketing use, we will delete/anonymize your personal data when you opt-out of the marketing and sales communication or when we can no longer guarantee your data is still relevant or up-to-date. You can refuse to share your contact details or opt-out at any time by following the unsubscribe link in the e-mail or by filling out a web form on our website. Who uses your information? We, OneTrust LLC, use your data, and may also share your personal data with our parent companies, subsidiaries and/or affiliates for purposes consistent with the OneTrust Privacy Notice. How do we share and disclose information to third parties? We do not rent or sell your personal data to anyone. We may share and disclose information (including personal data) about our customers in the following limited circumstances: 1. Vendors, consultants and other service providers: We share your information with third party vendors, consultants and other service providers who we employ to perform tasks on our behalf. These companies include (for example) our payment processing providers, website analytics companies (e.g., Google Analytics), CRM service providers (e.g., Salesforce), email service providers (e.g., Sendgrid) and others. Where OneTrust receives your personal data and subsequently transfers that information to a third party agent or service provider for processing, OneTrust remains responsible for ensuring that such third party agent or service provider processes your personal data to the standard required by the GDPR (and any other applicable privacy laws). For transfers of personal data from the EEA (or the UK) to the United States and other non-EU countries, OneTrust relies on Standard Contractual Clauses

issued by the European Commission (please refer to the section 'International Data Transfers' of our online Privacy Notice for further details).

2. Business Transfers:
We may choose to buy or sell assets, and may share and/or transfer customer information in connection with the evaluation of and entry into such transactions. Also, if we (or our assets) are acquired, or if we go out of business, enter bankruptcy, or go through some other change of control, personal data could be one of the assets transferred to or acquired by a third party.

3. OneTrust Group Companies:
We may also share your personal data with our parent companies, subsidiaries and/or affiliates for purposes consistent with this information and OneTrust Privacy Notice.

4. Protection of OneTrust and Others:
We reserve the right to access, read, preserve, and disclose any information as necessary to comply with law or court order; enforce or apply our agreements with you and other agreements; or protect the rights, property, or safety of OneTrust, our employees, our users, or others.

5. Disclosures for National Security or Law Enforcement:
Under certain circumstances, we may be required to disclose your personal data in response to valid requests by public authorities, including to meet national security or law enforcement requirements.

How to exercise your data subject rights?
Please be advised that under the GDPR you have the right to correct inaccurate personal data or complete your personal file, erase your data that we hold, as well as restrict or object to our processing. If you would like to exercise any of your rights, you can either click the “Exercise Your Rights” link available on the top right of OneTrust Privacy Notice, or fill out this web form directly. Our privacy team will examine your request and respond to you as quickly as possible. Finally, you also have the right to lodge a complaint with the relevant Data Protection Authority.

Your access request is now closed. For further information on your rights, our ways of processing personal data and security safeguards involved, please consult OneTrust Privacy Notice available online at https://www.onetrust.com/privacy-notice/.

If you have any additional questions, please do not hesitate to get in contact with us.

Thank you,
OneTrust Privacy Team

Reply from data subject:

Dear Privacy team,

Thank you for your information.

I must say that I find it quite vague for a company specialising in privacy.

I would like to precisely now, where my data actually went, and not hypothetically (" We may also share your personal data with our parent companies, subsidiaries and/or affiliates for purposes consistent with this information and OneTrust Privacy Notice.": which ones were actually shared and for what ?)

Also, I would like to know on which basis you transfer my data to the US (CCT ? BCR ?) and you to provide me with a copy of the relevant document.

This is also an obligation under Article 15.

Best regards,

XXXXX

Response from controller:

XXXXX,

Thank you for reaching out, please find below the response to your questions:

Recipients/Categories of Recipients to whom your personal data has been disclosed:
Controllers – your personal data was not shared with any other data controllers besides us (OneTrust LLC).
Processors – your personal data was shared with our data processors that are our technical service providers for the following types of tools and services:
CRM software (Salesforce)
Email Campaign and event management software (Eloqua, Cvent)

The details of how your personal data was transferred to third countries and information about the appropriate safeguards relating to the transfer:
Your personal data was transferred outside the EU to the following countries: United States of America (US) and United Kingdom of Great Britain and Northern Ireland (UK).

Transfers to the UK – according to the Withdrawal Agreement between the UK and the EU, a transition period currently applies during which the EU laws (including the GDPR) apply to the UK in the same manner as prior to the country's exit from the EU,Transfers to the US – your personal data was transferred to the US under the Privacy Shield Framework. As the Privacy Shield has since been invalidated by the CJEU as a personal data transfer mechanism, we will not be relying on it for any future transfers of your personal data from the EU into the US (should they occur).

If you would like to learn more about which appropriate safeguards we currently rely on for our international data transfers, please kindly refer to the section International Data Transfers of our online Privacy Notice.

If you have any additional questions, please do not hesitate to get in contact with us.

Kind regards,
OneTrust Privacy Team

	Reply from data subject: Dear Sir/Madam, Could I have the precise information request as to : • whether my data re sent to the US ot not ("transfer, should they occur" is not a showing accountability when it comes to knowing where the data are communicated by OneTrust to third parties) • On which legal basis is the transfer taking place ? (instead of thelegal basis on which the transfers are NOT taking place). Thank you for providing such an answer before end of the week. Should it not be the case, I intend to file a complaint with the competent DPA. Best regards, XXXXX --- **Response from controller:** XXXXX, Please find below the answers to your questions: • "whether my data re sent to the US ot not ("transfer, should they occur" is not a showing accountability when it comes to knowing where the data are communicated by OneTrust to third parties)" o Yes, your data was sent to the US – please see our previous email to you (from August 6th) for more detailed answer on this. o Please note that as you did not attend our webinar and are not subscribed to our marketing emails, we do not anymore process your personal data (outside of our current interaction and your previous DSAR request). • "On which legal basis is the transfer taking place ? (instead of the legal basis on which the transfers are NOT taking place)." o Back when we transferred your personal data into the US (in context of your webinar registration), we relied on the EU-US Privacy Shield framework – this was prior to the CJEU Ruling in Case C311/18. o After the CJEU Ruling, we have been relying on Standard Contractual Clauses and a set of supplemental measures to protect privacy and security of the processed personal data. We have also been continually monitoring the circumstances of the EU-US transfers in order to ensure that these maintain, in practice, a level of protection that is essentially equivalent to the one guaranteed by the GDPR. If you would like to learn more about which appropriate safeguards we currently rely on for our international data transfers, please kindly refer to the section International Data Transfers of our online Privacy Notice. Kind regards, OneTrust Privacy Team

Revolut	Claim that they rely on Standard Contractual Clauses.
Data subject 1	**Response from controller:** Dear XXXXX, Thank you again for getting in touch on this issue. We appreciate you taking the time to do so. We are continuing to examine the recent decision of the Court of Justice of the European Union ("CJEU") that impacts how EU personal data can be transferred internationally. We take our privacy and data protection obligations very seriously. In the meantime, we can provide the following answers to your questions: • We process and store the vast majority of our customers' personal data within the United Kingdom and European Union. However, Revolut does transfer a limited amount of customers' personal data outside of the United Kingdom and European Union. Further details are set out at Section 12 of our Customer Privacy Policy. • Where customers' personal data is transferred from the United Kingdom or European Union, transfers are carried out in accordance with GDPR Chapter 5 (Transfers of personal data to third countries or international organisations). In particular, we ensure that: • we transfer personal data to third countries that the European Commission has determined provide an adequate level of protection for exported personal data as required by GDPR Article 45 (Transfers on the basis of an adequacy decision); or • where we transfer personal data to a third country that does not have an adequacy decision, we only transfer personal data where suitable safeguards are applied under GDPR Article 46 (Transfers subject to appropriate safeguards); or • where we transfer a limited amount of personal data on a one-off basis, we may rely on a derogation set out under GDPR Article 49 (Derogations for specific situations) (for example, the transfer is necessary to establish, exercise or defend legal claims). • On foot of the CJEU's recent decision, we are examining our international transfers to ensure that no transfers to the United States of America continue under the auspices of the Privacy Shield. Where transfers were previously legitimised under Privacy Shield, we are ensuring that appropriate alternative safeguards are put in place (for example, standard contractual clauses, if appropriate). • We do rely on standard contractual clauses for a limited number of international transfers. We are currently examining our contract ecosystem to ensure that we can provide customers with copies of relevant standard contractual clauses. Thank you, again, for getting in touch with us about this. We will be back in touch to follow up with copies of relevant standard contractual clauses. In the meantime, we hope you continue to enjoy using Revolut. We care deeply about customer satisfaction. However, you have the right, at any time, to make a complaint to the Information Commissioner's Office Kind regards

Signal	Did not respond to specific questions regarding data transfers.
Data subject 1	**Response from controller:** Hello, Thank you for contacting us. Signal is committed to protecting the privacy and security of your data. Signal is specifically designed to minimize the data needed to deliver our service. All message contents and calls are end-to-end encrypted, so we cannot access them or provide them to anyone else. No party can intercept your messages or calls. Signal stores the minimum information required for you to send and receive messages on your devices. That information includes your phone number (which you provided in order to sign up for Signal), and end-to-end encrypted data, which we cannot access, in order to support the app's functionality. Because we cannot decrypt your data, the only place to view this personal information is on your own device. Signal uses cloud providers like AWS that utilize servers across the globe to help ensure that calls and messages are routed and delivered quickly and efficiently. Signal does not operate its own data center, as is common for apps. We've designed Signal to keep your data in your hands rather than ours. You can read more about how we think about concepts like privacy, security and trust here: https://signal.org/blog/looking-back-as-the-world-moves-forward/. I hopethis provides you with the information you need. Signal is an independent nonprofit and we rely on the support of our community. If you find the service useful, please consider making a donation today: https://signal.org/donate/ Thank you, Signal Privacy

Slack	Claim that they do not voluntary transfer data to governments do not provide data under Executive Order 12333.
Data subject 1	**Response from controller:** Hi XXXXX, Thank you for reaching out. We reviewed the Court of Justice of the European Union's judgement, and are confident that we can continue business as usual, relying on other legitimate methods of transferring data between the European Union and the United States. We provide support to our customers for compliance with international data transfers by executing Standard Contractual Clauses through our Data Processing Agreements. For more information, you can find Slack's Data Processing Agreements at this link: https://slack.com/intl/en-ie/terms-of-service/data-processing Slack takes the protection of your personal information very seriously. Slack does not voluntarily provide governments with access to any data about users for surveillance purposes. See our Privacy Policy, Data Request Policy, and Slack's Transparency Report for more information on the measures we put in place to protect your company from unlawful surveillance and disclosure of personal information.

	The focus of Slack's security program is to prevent unauthorized access to customer data and we're committed to being transparent about our security practices and helping you understand our approach. Please see Slack's Security Whitepaper for more information on encryption standards and other technical and organizational measures in place. Please also note that Slack has a number of features to allow more granular control and access to your data including: • Enterprise Key Management: Complete control and visibility of access to your data in Slack using your own encryption keys. Available on Enterprise Grid. • International Data Residency: Slack's data centers are hosted globally, with Amazon Web Services (AWS). The data center hosting location applicable to each Slack customer can vary if the organization uses our data residency feature. Data residency for Slack allows global teams to choose the region where certain types of data at rest are stored while fulfilling corporate policies and compliance requirements. Available on Plus and Enterprise Grid plans. Let us know if you have any further questions. Best, Privacy at Slack --- **Reply from data subject:** Hi XXXXX, Thanks for your email. Please can you let me know if FISA702 applies to you? Best, XXXXX --- **Response from controller:** Hi XXXXX, The Foreign Intelligence Surveillance Act is a United States federal law. To learn more about how Slack does not voluntarily provide governments with access to any data about users for surveillance purposes, I encourage you to review our Data Request Policy. Best, Privacy at Slack --- **Response from data subject:** Hi XXXXX, Please can you let me know if you involuntarily provide governments access to any data about users for surveillance purposes? Thanks, ---

	Response from controller: Hi XXXXX, It's XXXXX here stepping in for XXXXX. Following on from your question, I wanted to let you know that Slack takes the protection of your personal information very seriously. Slack does not voluntarily provide governments with access to any data about users for surveillance purposes. Please refer to our Privacy Policy, Data Request Policy, and Slack's Transparency Report for more information on the measures we put in place to protect your company from unlawful surveillance and disclosure of personal information. I'd also suggest reviewing the following blog post on international data transfers: https://slackhq.com/a-note-to-our-customers-on-international-data-transfers All the best, --- **Response from data subject:** Hi XXXXX, Thanks for your answer. Please let me know if Slack *involuntarily* provides data to governments for surveillance purposes. In other words, are you subject any orders that require you to or have ever required you to do this? Thanks, --- **Response from controller:** Hi XXXXX, Please note that Slack does not and cannot conduct real-time surveillance of customers, nor would we take action under Executive Order 12333. Let me know if you have any further questions. Best,

Tinder	Claim that they rely on Standard Contractual Clauses.
Data subject 1	**Response from controller:** Dear XXXXX, Thank you for contacting us. We take the privacy of our users very seriously and fully appreciate that the recent Court of Justice for the European Union's ruling on transfers of personal data to the USA (Case C-311/18 -- Data Protection Commissioner v Facebook Ireland and Maximillian Schrems) raises many questions for our users, just like it raises many questions for companies and regulators in general.

	We have worked to answer all of your questions below in line with our clear commitment to transparency and advise that in light of the recent Schrems decision, we are also working diligently and swiftly to review the situation and our practices in light of the emerging and anticipated guidance from EU data protection authorities and the European Data Protection Board as it becomes available. We may thus provide additional updates from time to time. 1. Do you transfer data outside of the EU? If yes, to which countries? 2. Yes, to the United States. 3. What is the legal basis relied on for each transfer (e.g. adequacy decision, SCCs, BCRs, derogations...)? If you used SCCs or BCRs, please provide a copy of the SCCs or BCRs used for each transfer. 4. Depending on the vendor, the legal basis relied on for the transfer of data to our vendors may be standard contractual clauses, Binding Corporate Rules or Privacy Shield. Where standard contractual clauses are used, we use the Controller to Processor SCCs approved by the European Commission in Decision 2010/87/EU, which are available from the following link: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en. We are in the process of reviewing transfers to our vendors and associated legal basis and, where relevant, we are implementing appropriate updates in light of the recent ruling. In doing so, we are taking account of the initial guidance issued by the European Data Protection Board on 24 July 2020. We will also be adapting our arrangements to the extent it may be necessary to reflect the future EDPB Guidance on this issue which is expected to be available shortly and we are continuing to monitor related matters on an ongoing basis e.g. the Commission's proposal to update the SCCs for GDPR purposes and the discussions between the US and the EU in relation to a possible replacement for the Privacy Shield. 1. If you send personal data to the US, do any of your partners fall under 50 USC §1881a ("FISA 702") or provide data to the US government under EO 12.333? To our knowledge, we have never received any FISA 702 requests or provided any data to the US government under EO 12.333. Like all other responsible controllers, we are reviewing our data transfer arrangements with vendors in light of the recent Judgment in Case C-311/18 and the emerging and anticipated guidance from the EDPB and the EU Commission. 2. If you send personal data to the US, which technical measures are you taking so that my personal data is not exposed to interception by the US government in transit? See our response to Question 3 above. 3. If you transfer personal data to a US-based "electronic communication service provider" as defined in 18 U.S. Code §1881(4)(b), or, should you still rely on the Privacy Shield for such transfer, I request that you stop the transfer of my personal data immediately. Given the recency of the Court of Justice for the European Union's ruling on transfers of personal data to the USA, at this time, it is not possible for us to provide the Tinder service without transferring data to the USA. As indicated above however, we are in the process of reviewing transfers to vendors and the associated legal basis in light of the recent ruling and the emerging regulatory guidance. You can delete your account at any time within the app by tapping the profile icon, go to "Settings," scroll down and select "Delete Account." You'll see a message that says "Account successfully deleted. Kind Regards

Trivago	Claim that they rely either on Article 49 GDPR derogations, or Standard Contractual Clauses, for transfers.
Data subject 1	**Response from controller:** Sehr XXXXX; hiermit kommen wir auf Ihre Anfrage vom XXX XXX zurück und können Ihnen auch ohne eindeutige Identifikation der durch Sie vollzogenen konkreten Nutzungshandlungen bereits die folgende Auskunft bzgl. Ihrer Fragen erteilen: I. „Übermitteln Sie Daten außerhalb der EU? Wenn ja, in welche Länder?“ Ob und in wie weit Trivago personenbezogene Daten auch außerhalb der EU übermittelt, hängt vom jeweiligen Einzelfall ab. Im Falle von Buchungen für Destinationen außerhalb der EU werden personenbezogene Daten an die entsprechend gebuchten Unternehmen oder deren Dienstleister wie Hotels oder Reiseagenturen zur Durchführung der Buchung übermittelt. Trivago selbst setzt außerdem für die Abwicklung seiner Dienstleistungen und Plattform Dienstleister u.a. in Israel, England und den USA ein. Auch hier können im Einzelfall personenbezogene Daten von diesen Dienstleistern verarbeitet werden. Welcher Dienstleister im jeweiligen Einzelfall eingesetzt wird, muss konkret ermittelt werden – dies kann erst nach einer eindeutigen Identifikation Ihrer Nutzungen durch Trivago geleistet werden. II. „Auf welche Rechtsgrundlage stützt sich diese Übermittlungen (z.B. Entscheidung über die Angemessenheit, SCCs, BCRs, Ausnahmen…)? Wenn Sie SCCs oder BCRs verwendet haben, legen Sie bitte für jede Übertragung eine Kopie der verwendeten SCCs oder BCRs vor.“ Je nach Einzelfall kommen verschiedene Rechtfertigungstatbestände bzw. Berechtigungen oder eine Kombination derselben für die Übermittlung von personenbezogenen Fragen außerhalb der EU bei Trivago zum Einsatz. Übermittlungen können auf Angemessenheitsentscheidungen, Standardvertragsklausel oder Ausnahmen gem. Art. 49 DSGVO gestützt sein. Sofern Standardvertragsklauseln zum Einsatz kommen, werden die unter https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087 sowie https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D0915 auffindbaren Klauseln verwendet. „Binding Corporate Rules“ kommen bei Trivago nicht zum Einsatz. Eine Auskunft des Einzelfalls sowie der entsprechenden Rechtsfertigungstatbestände kann leider erst nach einer eindeutigen Identifikation Ihrer Nutzung durch Trivago erfolgen. III. „Wenn Sie personenbezogene Daten in die USA übermitteln, fällt einer Ihrer Partner unter 50 USC §1881a („FISA 702“) oder stellt er der US-Regierung Daten gemäß EO 12.333 zur Verfügung?“ Eine pauschale Beantwortung dieser Anfrage ist so nicht möglich. Für konkrete Einzelfälle bzgl. Ihrer personenbezogenen Daten bedarf es zunächst einer eindeutigen Identifikation Ihrer Nutzungen durch Trivago. IV. „Falls Sie personenbezogene Daten in die USA senden, welche technischen Maßnahmen ergreifen Sie, damit meine personenbezogenen Daten während der Übermittlung nicht von der US-Regierung abgefangen werden?“ Die jeweiligen getroffenen technischen Maßnahmen richten sich nach einer Risikoabwägung im jeweiligen Einzelfall. Eine pauschale Beantwortung dieser Frage ist so ebenfalls nicht möglich. Für konkrete Einzelfälle bzgl. Ihrer personenbezogenen Daten bedarf es zunächst einer eindeutigen Identifikation Ihrer Nutzung durch Trivago.

	Sofern Sie eine weitergehende Auskunft bezüglich Ihrer Fragen von uns erhalten wollen, bedarf es zunächst einer eindeutigen Identifikation der durch Sie vollzogenen konkreten Nutzungshandlungen durch uns. Hierfür benötigen wir Ihre E-Mail-Adresse, die Sie im Rahmen Ihres Trivago-Accounts bei uns registriert haben. Wir werden Ihnen sodann eine E-Mail zur Bestätigung Ihrer Identität an diese E-Mail-Adresse zu kommen lassen. Bei Fragen stehen wir Ihnen gerne zur Verfügung. Mit freundlichen Grüßen,

Twitter	Claim that they rely on Standard Contractual Clauses.
Data subject 1	**Response from controller:** Hello, Thank you for contacting us. On July 16, the European Court of Justice (ECJ) invalidated the Privacy Shield framework, one of the legal structures that enabled companies to lawfully transfer personal data from the EU to the U.S. Twitter has appropriate legal mechanisms and safeguards in place to enable it to continue to transfer data to the U.S. Specifically, Twitter has long had Standard Contractual Clauses (SCC's) in place to provide a secondary lawful transfer mechanism. We trust this answers your question. Best, Twitter

Under Armour	Referred the data subject to their privacy policy.
Data subject 1	Dear XXXXX, Thank you for reaching out, your message is important to us! MyFitnessPal is operated by Under Armour, Inc. Therefore, when you sign up and use MyFitnessPal, your data is transferred to the US to enable us to provide the Services outlined in our Terms. It is important to us that our European users are aware of this. Therefore, as an EU user, when signing up for MyFitnessPal, you were asked to consent to several distinct items, including the transfer of your data to the US and your agreement to our Privacy Policy and Terms. Without this consent to the transfer of your Personal Data to the US, the app cannot operate and provide you its features. In this notice, we inform you that laws in the U.S. may be viewed as less protective than those of your country or region. However, this does not mean that Under Armour is treating your data with any less protections when it is handled in the US and Under Armour seeks to apply the standards laid out in the General Data Protection Regulation and other similar laws globally throughout its consumer journey. In order for us to provide the Services to you, we engage third party service providers who store and otherwise process personal data on our behalf. Many of these service providers are based in the US. Data transferred to our third party service providers is encrypted in transit and require our third party service providers to implement encryption technologies. In light of the recent Schrems II decision (C-

	311/18), we are also working to ensure that any transfer of data to those third party service providers remains subject to a valid export mechanism. You can find more information on our data collection and processing activities in the Location-Specific Disclosure section of the Privacy Policy. Please select the 'Read More' link next to 'Residents of the European Economic Area and the United Kingdom'. These additional resources may also be of use to you: · For information on the categories of personal data collected and the purposes for data processing, please read the How We Collect and Use Personal Data section of our Privacy Policy. · Please see the How We Disclose Personal Data section of the Privacy Policy to learn more about how and why personal data may be disclosed. A list of the types of companies Under Armour shares data with can also be found here. · Information about our data retention practices can also be found in our Privacy Policy. Thank you, UA Privacy

Virgin Media	Claim that they rely on Standard Contractual Clauses.
Data subject 1	**Response from controller:** Dear XXXXX Further to your request dated XXX XXX on international data transfers, please find our response below. Our records confirm that you are a current Virgin Media broadband customer. We also confirm that you were previously a TV customer. Our investigation to confirm whether we continue to process your personal data with respect to your previous TV account is ongoing. We have therefore answered the questions in your request in the context of the processing of personal data as part of the delivery of our broadband services. Transfers of personal data outside of the EU In order to deliver our broadband services, personal data is transferred to the following countries outside of the EU: India and the Philippines for the purposes of account management and customer care activities (including billing, technical support and sales purposes). We rely on Standard Contractual Clauses for the transfers. Please find attached the Standard Contractual Clauses that are currently available for disclosure. We can confirm that Virgin Media does not transfer personal data to the United States as part of the delivery of its broadband services. As regulatory guidance and advice becomes available in relation to international data transfers following the Schrems II judgment, we will take steps to react to it promptly. We hope this helps and provides the information you require for now. Please do not hesitate to contact us should you require any further information or clarification on our response. Kind regards,

WhatsApp	WhatsApp did not provide a response to this request.
Data subject 1	**Request from data subject:** *Dear Sir/Madam,* *I am one of your customers. In accordance with Articles 12, 13, 14 and 15 of the GDPR, I make the following requests:* • *Do you transfer data outside of the EU? If yes, to which countries?* • *What is the legal basis relied on for each transfer (e.g. adequacy decision, SCCs, BCRs, derogations...)? If you used SCCs or BCRs, please provide a copy of the SCCs or BCRs used for each transfer.* • *If you send personal data to the US, do any of your partners fall under 50 USC §1881a ("FISA 702") or provide data to the US government under EO 12.333?* • *If you send personal data to the US, which technical measures are you taking so that my personal data is not exposed to interception by the US government in transit?* *Please reply within one week as the GDPR requires you to reply 'without undue delay'. This is a simple request that does not require extensive analysis. Further identification beyond my email does not seem necessary given that I do not demand a copy of my personal data. Should you require any further information, please do not hesitate to contact me.* *Regards,* **No response from controller.**

Zoom	Claim that they rely on Standard Contractual Clauses, and are offering users to sign them.
Data subject 1	**First response from controller:** Dear XXXXX, We note that you've emailed us from an address that is not associated with your organisation. Would it be possible to please send us an email from the XXX domain to confirm that you are indeed associated with that account? Following receipt of that email, we will respond as quickly as we can. Kind regards, --- **Second response from controller:** Dear XXXXX, First, please allow me to apologize for the delay. We have received a number of questions like yours from our E.U.-based customers since the Schrems II decision. Questions like: · How does the Schrems II ruling affect my use of Zoom? · How can E.U. companies transfer data to Zoom in the U.S.? · Does Zoom offer the E.U. Standard Contractual Clauses (SCCs)? · Does Zoom give user information to the U.S. Government? · Is Zoom subject to s. 702 FISA or to EO12333? We've attached an FAQ that addresses those and more. Like every U.S.-based provider of cloud technology services, Zoom is reviewing the CJEU's ruling to consider whether we need to take additional measures over and above our existing data export compliance mechanisms. We will continue to monitor for any guidance or regulations that might affect our offerings.

	Zoom customers can continue to transfer data to the U.S. from the EEA/UK under the Standard Contractual Clauses (SCCs), available here. Our intention is for all of our customers to have the benefit of the DPA and SCCs whenever they use Zoom. Going forward, however, EU regulators may not consider the SCCs valid unless they are actually signed by both parties. That's why we are also making the pre-signed SCCs available to any user who wants to sign them. It's your choice whether or not you'd like to sign them, and you can do so at any time. If you wish to submit a signed copy of Zoom's SCCs, please submit them to privacycontracts@zoom.us. If you are submitting a signed DPA and Exhibit D (SCCs), please send that to your Account Executive. For additional information about how we evaluate and process government requests from around the globe, please see our Government Requests Guide: https://zoom.us/docs/en-us/government-requests-guide.html. Best Regards,