Information Commissioner's Office SendGrid (cloud-based email service)

Transfer Risk Assessment (TRA)

Status: Official

VERSION HISTORY

Version Number	Changes since last version	Status	Date	Author(s)
0.1	Initial draft	Draft	27/07/22	[redacted]
0.2	Second draft	Draft	03/08/22	[redacted]
0.3	Final version	Final	10/10/22	[redacted]

CONTENTS

Step 1: Can you satisfy the key requirements under the UK GDPR?

Satisfaction of the key requirements of the UK GDPR

Background for TRA

Since 2018, the Information Commissioner's Office (**ICO**) has used SendGrid (a cloud-based email service) to help manage its email services and to offload the creation and sending of emails, removing the need to run its own email infrastructure. The ICO uses SendGrid for sending emails comprising alerts such as success/failure messages, and for sending the outputs of web forms as emails from the ICO website to itself, to the ICO's casework systems. SendGrid uses Amazon Web Services (**AWS**) network infrastructure. SendGrid is hosted in an AWS datacentre in the US.

Twilio (the parent company of SendGrid) recently updated its Data Protection Addendum (**DPA**) to incorporate new EU standard contractual clauses (**SCCs**) to "*provide an updated data transfer mechanism for personal data transfers originating from the EEA and better align them with the requirements of the GDPR*".

SendGrid is currently only used by the ICO to send emails from the website to the ICO (for example service alerts, and the contents of web forms so they can be processed by ICO teams) (**website use-case**). In addition, the ICO is planning to use SendGrid instead of Outlook, to send registration and casework emails to its customers (**ICE use-case**).

The *Schrems II* judgment of 16 July 2020 has received significant press attention and impacts on the use of SCCs and other appropriate safeguards to legitimise transfers of personal data to the US. The judgment confirms that a TRA should be conducted in order for SCCs (or other appropriate safeguards) to be relied on for transfers to any third country, to consider whether the use of the appropriate safeguards for transfers to that third country will provide an "essentially equivalent" level of protection of personal data.

The ICO operates as the data exporter, transferring personal data from the UK to SendGrid (US-based), who in turn engages AWS as its US-based sub-processor. SendGrid is the data importer. Twilio (the parent company of SendGrid) has conducted its own TRA for these transfers.

This TRA is being conducted due to the fact that the location of processing the personal data for SendGrid is AWS' data centre in the US. As such, this TRA focuses on the UK to US data transfers.

Transfers to the US

SendGrid is hosted in AWS' data centre in the US, and therefore data is stored on servers located within the US.

There are some elements of the service which are sub-contracted by SendGrid to AWS who in turn operate as a sub-processor of the personal data, as follows:

Sub-Processor	Applicable Service(s)	Subject Matter	Nature and Purpose of Processing	Location(s) of Processing	External links for additional information relating to security
AWS	Email (SendGrid)	Personal data contained in email communications.	Routing and transmission of emails.	USA	Compliance Program; GDPR Centre; Supplementary Measures Addendum; Blog

Satisfaction of key UK GDPR obligations

The key principles of data minimisation, security, lawful basis, controller to processor obligations and transparency are satisfied. In order to enhance the transparency position, the ICO could notify those customers whose data will be shared with SendGrid (or SendGrid's sub-processors) in the US (to be clear, this is not because their consent is required, more as a matter of courtesy and to give people an opportunity to raise any concerns that they might have) – most likely via an amendment to the online privacy notice.

Is this TRA tool suitable for your transfer risk assessment?

Yes – this TRA tool is suitable for the personal data transfer for the reasons outlined below:

- The transfer is not covered by adequacy or an exception, and the transfer does not involve more than one country's law (only the US).
- The transfer is not to a country with poor human rights record.
- The transfers are not too complex to invalidate the use of this TRA tool. The services delivered by SendGrid are very commonly delivered via cloud solutions – by SendGrid and other suppliers – and this may involve the processing of personal data in the US. The risks around these restricted transfers are not too high to invalidate this tool.
- Twilio's DPA states that for transfers of personal data to a country outside the EEA, the SCCs shall apply, and for transfers of personal data outside of the UK, the UK International Data Transfer Agreement (**IDTA**) shall apply. Please note that while Twilio remains certified under the EU-US Privacy Shield, the decision in *Schrems II* declared the EU-US Privacy Shield as invalid – therefore Twilio relies on SCCs and the UK IDTA to enable lawful transfers of data internationally.

Record the specific circumstances of the transfer

Where is the data going (plus controller/processor status)? (eg a public regulator like the ICO, an IT company, a parent or service company in your group). Is the importer a controller, joint controller, processor or sub-processor?

The ICO is the data controller, and SendGrid is the processor. The ICO operates as the data exporter, transferring personal data from the UK to SendGrid (US-based), who in turn engages AWS as its US-based sub-processor. SendGrid is the data importer.

Where is the importer located?

The US.

Will the importer be making any onward transfers?

None are intended.

Why is the transfer being made and what will they be doing with the personal data?

The transfer will enable the ICO to exercise its official authority and carry out its public tasks, including providing a complaints service, and providing a service for data controllers to register and pay.

The use of an SMTP service is needed to offload the creation and sending of emails, removing the need to run the ICO's own email infrastructure.

Categories of the personal data and data subjects

Personal data that is typically processed in the provision of the services from SendGrid is set out below:

In relation to the website use-case, as follows:

- ***Service alerts*** – (1) *Categories of data:* Email address of recipient(s). (2) *Data subjects:* ICO website alert recipients (selected ICO staff).
- ***Web form data, e.g. forms for complaints, registration, breach reporting, requesting a speaker*** – (1) *Categories of data*: Email addresses, contact details, names, details of what the organisation did or didn't do, details of a breach, copies of correspondence between a complainant and an organisation. (2) *Data subjects*: Complainants, organisations being complained about, controllers, ICO website service users.
- ***Account management*** – (1) *Categories of data*: Names, email addresses. (2) *Data subjects*: ICO staff contacts responsible for the management of the SendGrid subscription.

In very limited circumstances, special category data could be included in a minority of emails. This could include for example health or criminal offence data, in cases where the ICO is corresponding with a data controller to handle a complaint and such data is relevant to the complaint (and provided by the complainant to the ICO).

In relation to the ICE use-case, as follows:

- ***Registration emails*** – (1) *Categories of data*: organisation name, organisation address, any trading names, contact details (name, emails and postal address), information about the fee tier being paid (number of staff and turnover), Data Protection Officer (DPO) name and contact details, payment details for the processing of fees (e.g. for direct debit payments this will include sort code and account number with some number obscured), ICO staff name and work contact details. (2) *Data subjects*: main contact for registered organisations including sole traders, DPO contact for registered organisation, ICO staff, enquirers.
- ***Complaint emails*** – (1) *Categories of data*: any information within the ICO's care relating to casework processed through ICE 360 may include contact details (name, emails and postal address) and complaint details. When complainants describe their complaint and upload supporting evidence, this may include: date of birth, NI number, employment details, bank details (only min. details to allow identification), data breach descriptions, advice and information requests, data relating to criminal offences, staff name and work contact details, and other special category data. (2) *Data subjects*: complainants, enquirers, ICO staff, staff at other organisations, MPs.
- ***Spam reports*** – (1) *Categories of data*: spam reports, that may contain email content. (2) Data subjects: main contact for registered organisations including sole traders, DPO contact for registered organisation, ICO staff, enquirers, complainants, staff at other organisations, MPs.
- ***Account management*** – (1) *Categories of data*: Names, email addresses. (2) *Data subjects*: ICO staff contacts responsible for the management of the SendGrid subscription.

What technological and organisational security measures will the importer have in place?

See above.

The format of the data (plain text, pseudonymised or encrypted)

SendGrid supports the ability to enforce end-to-end TLS encryption, so that we can ensure that data contained within emails, including attachments, is appropriately secure.

How is the data transferred?

- Customers enter information into a form on the ICO website.
- Information passes through the Web Application Firewall, which checks the entries for malicious content (malicious content would be blocked) (existing).
- Information is stored temporarily in the website database in line with retention schedules (typically 14 days) (existing).
- The web application connects to SendGrid via an API key and passes data to be sent by email to SendGrid, which sends the email to the recipients, using a minimum of enforced TLS 1.2.

The SendGrid SMTP (Simple Mail Transfer Protocol) service functions as a method to send emails from one mail server (or mail client) to another across the Internet. When the ICO sends an email via SendGrid, the SendGrid SMTP server processes the email, decides which server to send the message to, and relays the message to that server. Data may be processed by SendGrid and its sub-processor AWS, located in the US, for routing and transmission of emails worldwide as may be necessary. However, the processing would only take place within the US, which is the focus of this TRA.

How long will the importer have access to the data?

SendGrid will process Customer Account Data as long as required to provide the services to the customer, for SendGrid's legitimate business needs, or by applicable law or regulation.

SendGrid stores minimal random content samples for 61 days. Any stored Customer Content (including on SendGrid's backup systems) is deleted one year after the termination of the contract. SendGrid will process Customer Account Data as long as required to provide the services to the customer, for SendGrid's legitimate business needs, or by applicable law or regulation.

How often will these transfers occur?

This is a bulk email service. The ICO will send many emails a day (up to 10s of thousands) using this service.

Step 2: Are the contractual safeguards likely to be enforceable in the destination country?

Are the contractual safeguards likely to be enforceable in the destination country? (If yes, skip to step 3)

The US does respect the rule of law and there is a process via the US courts under which foreign judgments/arbitration awards are recognised. It is a party to the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards. There is access to justice through the court system and independence in the judicial process.

As such, the contractual safeguards are likely to be enforceable in the destination country.

Step 3A: Is there an appropriate protection for the data from third-party access?

Is the destination country's regime similar enough to the UK's regime in terms of regulating third party access to data (including surveillance)? (If yes, then finish here)

As outlined in the *Schrems II* judgment, public authorities in the US do have wide powers to intercept communications and to access data from private companies, and the laws that allow this (i.e. s.702 FISA and Executive Order 12,333) are not subject to sufficient safeguards. The US does not have a comprehensive data protection law and generally does not have a comprehensive system which allows rights for an individual to pursue legal remedies in order to have access to personal data relating to them.

Ability to seek redress through the courts, particularly for non-US citizens, is also hampered by constitutional process. The third party access regime in the US does not provide appropriate legal protections/is not sufficiently similar to the principles which underpin the UK third party access regime.

Step 3B: What is the likelihood of third party access to the data?

How likely is the third party access to the data (including surveillance)? (If unlikely, then finish here)
For UK GDPR processing, if third party access to the data occurred (which is unlikely, particularly for the website use-case, as the data would be of no interest to US authorities or the surveillance community), the risk of harm to data subjects in relation to the website use-case would be low owing to the types of personal data being transferred to SendGrid/AWS (customer contact details, as well as customer ICO registration and case details). Although there may be health data and in limited circumstances criminal offence data, it will be of a domestic nature and therefore unlikely to be of any interest to US authorities, which further mitigates the risk. The processing would be unlikely to be processed by authorities in such a way that could cause major harm to individuals. In relation to the ICE use-case, despite the fact that some of the types of personal data being transferred are higher risk (e.g. bank details, data breach descriptions) than the website use-case, the risk of harm to data subjects would still be low due to the reasons set out above, albeit the risk is marginally higher than in the website use-case due to the fact that there may be some complaints which could potentially be of more interest to US authorities or the surveillance community (for example, if a complaint is in relation to a data breach or cyber-attack, and therefore attracts a higher interest threshold). In addition, SendGrid only retains data for limited time periods (see above) which means there would be a narrow window for requests to access the data. In any event, in the unlikely scenario that US authorities are interested in accessing the data, given the fact that the ICO is a UK public body and regulator, it is likely that such US authorities would approach the ICO directly or use diplomatic channels via the UK government to request access to such data, rather than approaching SendGrid or AWS, who would only be able to access encrypted versions of the data and who would likely object to releasing it. As above, the risk of harm to individuals would be low.

Step 3C: Considering the circumstances of the transfer and the destination country's regime, what is the risk of harm to data subjects?

Considering the circumstances of the transfer and the destination country's regime, what is the risk of harm to data subjects? (If low, then finish here)
As above, risk of harm to data subjects is low given the type of personal data involved and there is a low likelihood of third-party access to the data. The risk is also mitigated due to the fact that (1) even if US surveillance authorities were interested in accessing the data, it is likely that this would be requested via governmental/regulatory interaction, rather than via SendGrid/AWS; (2) the personal data involved is low-risk, and even where health data and in limited circumstances criminal offence data may be involved, it will be of a domestic nature, which means that it will likely be of no (or low) interest to US surveillance authorities; and (3) SendGrid only retains data for limited time periods (see above) which means there would be a narrow window for requests to access the data.

Step 4: Sign off and record outcomes

Role	**Name/position/date**
Digital Architect	[redacted], Digital Architect 10 October 2022
Conclusion: Given that we consider this to be a low-risk data transfer, we have conducted a fairly light-touch transfer risk assessment here but have documented it in a long-form TRA in order to take a robust approach and to ensure we have a sufficient audit trail.	