

Sendgrid Data Protection Impact Assessment

Document Name	Sendgrid (website) Data Protection Impact Assessment
Author/Owner (name and job title)	Greer Schick, Digital Architect
Department/Team	Digital and IT
Document Status (draft, published or superseded)	Draft
Version Number	V0.8
Release Date	28 March 2022
Approver (if applicable)	
Review Date	31 May 2022
Distribution (internal or external)	Internal

Privacy by design at the ICO

Welcome to the data protection impact assessment process. You should use this every time you want to implement or change a product or process. It is essential to managing your own project risks but also to managing the corporate risks of the ICO.

Responsibilities

It is your responsibility to ensure that data protection impact is taken into account during the design and build of your product or service. To do this successfully, you will need to be able to explain what your proposal is, and map out how data is used. This includes, amongst other things, where data might sit at any time geographically, but also the purpose of its use at different points in time.

Remember the basics. Key to a good assessment is knowing at all points in the process: what data you are collecting/using, why, where it will be stored and for how long, who will access it and why, how it will be kept secure and whether it's being transferred to any other country.

Your Information Asset Owner (your Director) is ultimately responsible for managing any residual risk once you have completed any mitigations to the risks you identify.

The Information Management Service, working on behalf of our DPO, can help complete the paperwork, provide compliance advice and spot risks. It is not the Service's responsibility to own, manage or mitigate the risks identified during the process.

Getting advice

You might also need advice from subject matter experts in other teams to make sure that you understand how something works or risks to what you are proposing to do. This is particularly likely if it involves new, or changing, technologies. Getting this advice will help to provide your IAO with assurance that you have understood and identified the risks.

You might well be working on a contract or agreement and a Security Opinion Report at the same time – these are also ways that you can mitigate risks and should be viewed as part of the overall assessment process.

The paperwork

You should think of this as a live document. You might change your plans or new information might come to light that changes the risk profile of your proposal. If that's the case, you should revisit the paperwork and update it to reflect any changes. You might also need to inform your IAO of new or changed risks.

The process

You should allow time for this process in your project plans. Start early! How long it takes will depend on what you're proposing, and how well you can explain it and identify risks. It can take several weeks to get the right advice and risk assessment in place.

Step 1

- Complete DPIA screening assessment. If you conclude that you do not need to complete a DPIA then you must make a record of your decision.
- If you do need to complete a DPIA then start completing the paperwork and notify the IM Service. Depending on what you're doing, the DPIA might need to be reviewed by the DPIA forum. You need to ensure the paperwork is sufficiently detailed, accurate and thorough before the forum is able to review it. This particularly applies to your descriptions of the processing activities you are proposing and how any associated technology works alongside it.
-

Step 2

- The forum is likely to provide advice and recommendations. You should consider this advice. If you decide not to follow it, then you must document your reasons why. If you do follow it, then most actions will need to be completed before go live. For example, updating privacy information or refining access controls.
- The forum is able to escalate risks to our Data Protection Officer and/or Risk and Governance Board if it is not comfortable with the processing activity being suggested or wants sign-off on advice.

When you have completed the DPIA paperwork and any actions, accepting that you might need to revisit it, you should get sign-off from your IAO before your product or service goes live.

If there are residual risks that your IAO would like to discuss, they can contact dpo@ico.org.uk. That discussion can be escalated to our Data Protection Officer and/or Risk and Governance Board if required.

Guidance for completing this template

Complete this Data Protection Impact Assessment (DPIA) template if your 'Screening Assessment - do I need to carry out a DPIA?' indicates a high risk to individuals. If you are unsure whether you need to complete a DPIA use the [screening assessment](#) first to help you decide.

Aim to complete your DPIA as early as possible as the outcome of the assessment could affect the viability of your plans. In extreme cases, you will not be able to continue with your plans without changing them, or at all.

Guidance notes are included within the template to help you with its completion- just hover your mouse over any blue text for further information.

The [Information Management Service](#) is also available for further advice and support. Please keep in mind our [service standards](#) if you require advice.

1. Process/system overview

1.1 Ownership

Project Title:	Sendgrid
Project Manager:	Greer Schick
Information Asset Owner:	Mike Fitzgerald
Controller(s)	ICO
Data processor(s)	DP: Twilio Sendgrid Sub processor: Full list of their sub-processors and assurance provided by Twilio here: Twilio Sub-Processors Amazon Web Services is the only sub processor identified for the Sendgrid service.

1.2 [Describe your new service or process](#)

The service being reviewed/implemented is Twilio Sendgrid. Sendgrid is a cloud-based email service.

Sendgrid is used to offload the creation and sending of emails, removing the need to run our own email infrastructure.

Sendgrid is already used by the ICO website. In relation to the ICO website, the purpose of this DPIA is to ensure that a DPIA has been completed for its continued use.

ICO website (existing)

The ICO website has used Sendgrid since 2018. It uses Sendgrid for sending emails comprising alerts such as success/failure messages, and for the sending the outputs of web forms as emails from the ICO website to ourselves, to our casework systems. There is *no proposed change* to the Sendgrid implementation for the ICO website.

A full DPIA was needed as the screening answered 'Yes' to the following questions:

- Will the processing involve [sensitive personal data](#) or data of a [highly personal nature](#)? For example, special categories of data (Article 9 refers), personal data relating to criminal convictions or offences (Article 10 refers), and personal data linked to household and private activities.
- Does the processing involve [large scale processing](#) of data at a regional, national or supranational level, and which could affect a large number of data subjects?

Scope

Inside scope

The scope of this DPIA is the use of Sendgrid by the ICO, to send emails from the website.

Outside scope

The *processing and management of data within the website service* is considered outside the scope of this DPIA (ie the creation, processing, and retention periods for data within the website are covered elsewhere and will not change as a result of this project).

1.3 [Personal data inventory - explain what personal data is involved](#)

1.3.1 Website

Categories of data	Data subjects	Recipients	Overseas transfers	Retention period
<p>Service alerts Email address of recipient(s)</p>	ICO website alert recipients (selected ICO staff)	<p>ICO website alert recipients (nominated IT staff who will receive email alerts about the website)</p> <p>Twilio / AWS</p>	Data may be processed by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.	Twilio will process Customer Account Data as long as required to provide the services to the customer, for Twilio's legitimate business needs, or by applicable law or regulation.
<p>Web form data, eg forms for complaints, registration, breach reporting, requesting a speaker</p> <p>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.</p>	<ul style="list-style-type: none"> Complainants Organisations being complained about Controllers ICO website service users 	<ul style="list-style-type: none"> ICO staff as applicable to the web form, eg case officers, registration team members, communications department team members Twilio / AWS 	As above	Sendgrid stores minimal random content samples for 61 days. Any stored Customer Content (including on Twilio's backup systems) is deleted one year after the termination of the contract.

1.3.2 General – covering ICO's use of the service

Categories of data	Data subjects	Recipients	Overseas transfers	Retention period
------------------------------------	-------------------------------	----------------------------	------------------------------------	----------------------------------

<p>Account management Names, email addresses</p>	<p>ICO staff contacts responsible for the management of the Sendgrid subscription</p>	<p>Twilio Sendgrid, Amazon web services.</p>	<p>Data may be processed by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.</p>	<p>Twilio will process Customer Account Data as long as required to provide the services to the customer, for Twilio's legitimate business needs, or by applicable law or regulation.</p>
---	---	--	--	---

1.4 [Identify a lawful basis for your processing](#)

Public task – Article 6(1)(e).

Special category data could be included in a minority of emails, and would include for example criminal offence data in cases where the ICO is corresponding with a data controller in carrying out its duty to collect the data protection fee, or other special category data where the ICO is carrying out its public task to handle complaints.

For special category data the lawful basis would be article 9(2)(g) substantial public interest and DPA schedule 1 paragraph 6 statutory and government purposes. The same processing condition is relied on for any data concerning criminal convictions and offences.

1.5 [Explain why it is necessary to process this personal data](#)

The processing is necessary in order for the ICO to exercise its official authority and carry out its public task, 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 our own email infrastructure.

Sendgrid was originally chosen for use by the ICO website in 2018 because it has strict anti-spam capabilities, and (unlike many other providers) offers sending from a dedicated IP address, both of which reduce the likelihood that the service is used by spammers and would result in ICO emails being refused or marked as spam or, at worst, blacklisted. Dedicated IP addresses additionally mean that ICO mail servers can easily be configured to recognise and route incoming emails from the service, mitigating the risk that our own email could be marked as spam or junk. Sendgrid also 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.

For the above reasons Sendgrid is recommended by Microsoft for sending emails from Azure web apps.

Sendgrid provides a simple SMTP relay option, as well as more advanced API integration that would support the ICO if we had future needs for sending emails from other applications.

Measures will be taken to minimise the personal data being processed by disabling tracking and analytics.

1.6 [Outline your approach to completing this DPIA](#)

Consultation has been undertaken with the Information Management team. Consultation is underway with Commercial Legal and TLT (external solicitors), in relation to international transfers.

Consultation with Cyber Security has taken place to complete both a supplier assurance assessment and SOR.

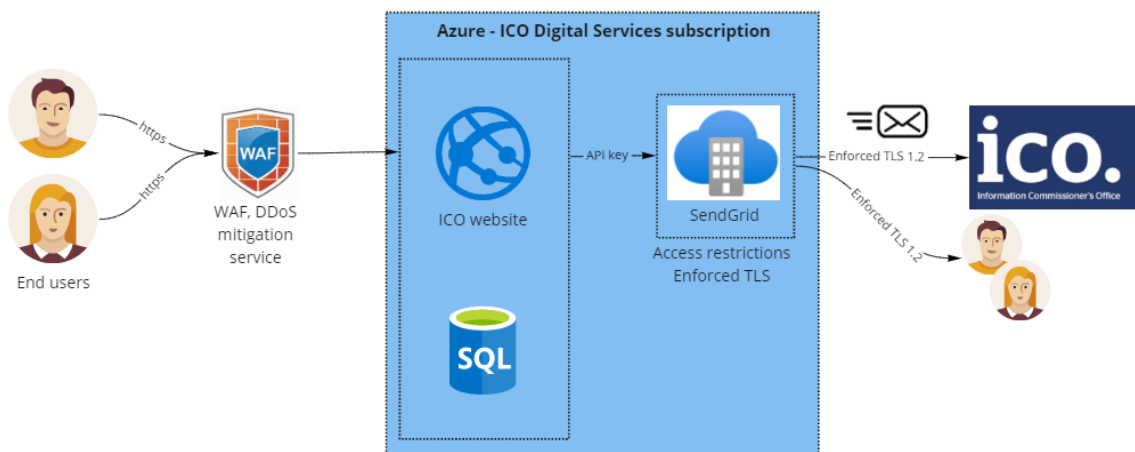
It was agreed that consultation with external data subjects will not be necessary as they are unlikely to be impacted by the ICO's choice of email service.

2.0 Data flows

2.1 Provide a [systematic description of your processing](#), from the point that the data is first collected through to its destruction.

If your plans involve the use of new technology you should explain how this technology works and outline any 'privacy friendly' features that are available.

High level Website



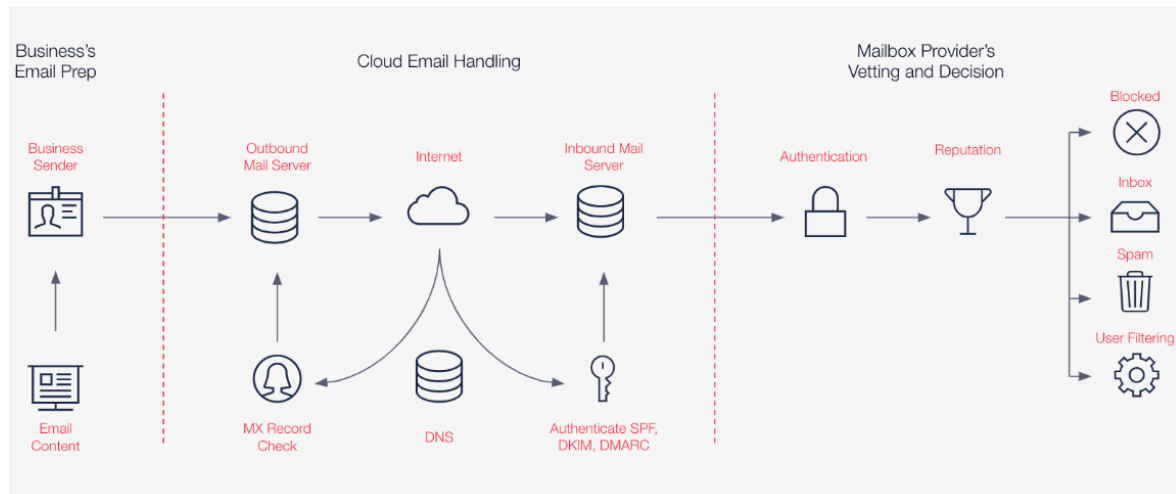
Description

1. Customers enter information into a form on the ICO website
2. Information passes through the Web Application Firewall, which checks the entries for malicious content (malicious content would be blocked) (existing)
3. Information is stored temporarily in the website database in line with retention schedules (typically 14 days) (existing)

4. 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.

In more detail ...

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:

1. The ICO application (website) makes an API call to the Sendgrid server.
2. Sendgrid verifies that the API username and API key used for authentication correspond to an active account
3. Sendgrid examines the incoming data to parse the message information, such as sender address, recipient, and message content.
4. The Sendgrid server takes the message information it gathered from our request and account settings (including analytics and TLS), and then repeats the process in Step 3 with the recipient's mail server.
5. The recipient's mail server checks the sending address, recipient address (to ensure they are a valid recipient), and message content. It checks the sending domain for any potential DNS issues, such as invalid DKIM and SPF signatures.
6. As long as there are no issues, the recipient's mail server will use the protocols POP3 or IMAP to retrieve the email and deliver the message to its intended recipient.

3.0 [Key principles and requirements](#)

Purpose & Transparency

1. Will you need to update our [privacy notices](#)?

Yes No

2. If you are not updating our privacy notices how do you intend to communicate information about your processing to the data subjects?

N/A

3. If [consent](#) is your lawful basis for processing personal data are you maintaining appropriate records of the data subjects consent?

Yes No N/a

4. If legitimate interests is your lawful basis for processing have you completed a [legitimate interest assessment](#)?

Yes No N/a

If applicable please provide a link to your completed assessment.

Accuracy

5. Are you satisfied the personal data you are processing is accurate?

Yes No

6. How will you ensure the personal data remains accurate for the duration of your processing?

Data is not being managed within the Sendgrid service; it is only used to process data sent to it by existing systems.

Where data is entered by users, there are existing safeguards to mitigate the risk of inaccurate data being entered, eg dual-entry email fields.

There are existing procedures in place to prompt and allow customers to update their data (contact details, for example), should it become inaccurate during its lifetime.

7. If the personal data isn't being obtained directly from the data subject what steps will you take to [verify accuracy](#)?

Personal data will be obtained directly from the data subject.

For information, testing has been carried out to ensure that data processed by the system is accurate, ie the same data that was sent to it.

Minimisation, Retention & Deletion

8. Have you done everything you can to minimise the personal data you are processing?

Yes No

9. How will you ensure the personal data are deleted at the end of the retention period?

A contract will be in place that sets out the retention periods which will be in line with what is detailed in section 1.3.

10. Will you need to update the [retention and disposal schedule](#)?

Yes No

Integrity and confidentiality

11. Where will the personal data be [stored](#)?

Data may be processed on Twilio's network infrastructure by Twilio and its sub-processor Amazon Web Services, located in the US, for routing and transmission of emails worldwide as may be necessary.

Spam reports, that may contain content, are kept indefinitely. Aggregated sending stats are kept indefinitely. Sendgrid stores minimal random content samples for 61 days. Any stored Customer Content is deleted one year after the termination of the contract.

12. Are there appropriate [access controls](#) to keep the personal data secure?

Yes No

Authorised ICO and support staff only have access to the Customer Account data, and Customer Content comprising recipient email address, and Customer Usage Data comprising metadata and sending statistics (number of emails sent, received, and opened) stored in Sendgrid. ICO staff will be authorised based on the principle of least privilege. In practice, it is expected that approx. 2-4 ICO individuals would have authorised access to Sendgrid.

Sendgrid has access controls in place including the principle of least privilege, regular access reviews, training, logging, password controls, multi-factor authentication, and password hashing. Twilio’s security overview, which includes the access controls included in the contract are available at <https://www.twilio.com/legal/security-overview>

13. Have you contacted the [cyber security team](#) for a security assessment of your plans?

Yes No N/a

14. Please explain the policies, training or other instructions you intend to put in place to enable staff to operate the new system or process securely.

Staff generally do not use the Sendgrid service directly. There’s no specific training required for ICO account management.

Accountability

15. Who will be the [Information Asset Owner](#) for this personal data?

Director of Digital, IT and Business Services

16. Will you need to update our [Article 30 record of processing activities?](#)

Yes No

17. If you are using a data processor have you agreed, or will you be agreeing, a written contract with them?

Yes No N/a

Individual Rights

18. Is there a means of providing the data subjects with [access](#) to the personal data being processed?

Yes No

A copy of email content that originates from ICE will continue to be held in ICE as per existing retention schedules.

Within the contract, Twilio commits to providing reasonable assistance to customers responding to requests from data subjects seeking to exercise its rights under applicable data protection laws, with respect to Customer Content processed by Sendgrid.

19. Can [inaccurate or incomplete](#) personal data be updated on receipt of a request from a data subject?

Yes No

Requests relating to inaccurate or incomplete personal data would be handled by existing processes, and would usually involve updating the details held on the ICE system (not Sendgrid).

20. Can we [restrict](#) our processing of the personal data on receipt of a request from a data subject?

Yes No

21. Can we [stop](#) our processing of the personal data on receipt of a request from a data subject?

Yes No N/a

22. Can we [extract and transmit](#) the personal data in a structured, commonly used and machine readable format if requested by the data subject?

Yes No N/a

23. Can we [erase](#) the personal data on receipt of a request from the data subject?

Yes No

Risk Description	Response to Risk	Risk Mitigation	Expected Risk Score		
			I	P	Total
			See Appendix 1 – Risk Assessment Criteria		
<p><i>Example:</i></p> <p><i>Access controls are not implemented correctly and personal data is accessible to an unauthorised third party.</i></p>	Reduce	<p><i>Existing mitigation: We have checked that the system we intend to procure allows us to set access permissions for different users.</i></p> <p><i>Expected mitigation: We will appoint and train a system administrator who will be responsible for implementing access controls and monitoring access. The system administrator will also audit the system periodically to review access permissions.</i></p>	3	2	6 - medium
Data is kept for longer than is necessary by data processor	Accept	Existing mitigation: Contract includes that data is processed only for as long as necessary: Spam reports, that may contain content, are kept indefinitely. Sendgrid stores minimal random content samples for 61 days. Any stored Customer Content (including on Twilio's backup systems) is deleted one year after the termination of the contract.	1	1	1
Individual rights - Data processed without regard for statutory rights.	Reduce	Existing mitigation:	2	1	2

		<p>Contract includes Privacy notice and Data Processing Addendum which includes commitments around providing "reasonable assistance" to helping customers respond to requests from data subject in line with their rights. [Noted that 'reasonable assistance' may leave some room for a residual risk]</p> <p>Contract also commits that subprocessors must meet the same standards of processing.</p> <p>In addition: Sendgrid provides a portal to configure settings for tracking and analytics, which include the ability to track if an email is opened and if links are clicked. These features will be disabled as part of implementation to minimise the personal data being processed.</p>			
Unauthorised access, destruction, loss, modification of data.	Reduce	<p>Existing Mitigation: Contract includes retention of information and details security to guard against unauthorised users accessing the system.</p> <p>In addition: Emails could be resent from the website content management system if an issue was reported and a request to resend was made within the retention period.</p> <p>Expected mitigation: Appropriate access controls will be implemented.</p>	3	1	3

Data processor network / system / online portal not secure	Reduce	Existing mitigation: Contract includes details of the security of the service. Expected mitigation: SOR to be completed giving assessment of the security of the service.	3	1	3
Data transferred overseas to a jurisdiction that does not adequately protect data subject rights	Accept	Existing mitigation: Contract, and Data Protection Addendum describe protections that are given for overseas transfers. Twilio state they rely on standard contractual clauses for the transfers. Commercial Legal have instructed TLT to prepare a Transfer Risk Assessment for the service.	2	1	2
Data processor fails to process data securely or in accordance with our instructions	Accept	Existing mitigations: Contract Supplier security assessment / risk assurance conducted by cyber security team.	3	1	3
Data is processed for unspecified / unlawful purposes/ not within expectations of data subjects	Accept	Existing mitigation: Assurance from Twilio they "do not sell your personal information, or the personal information of your end users. We also do not allow any personal information to be used by third parties for their own marketing purposes.."	2	1	2

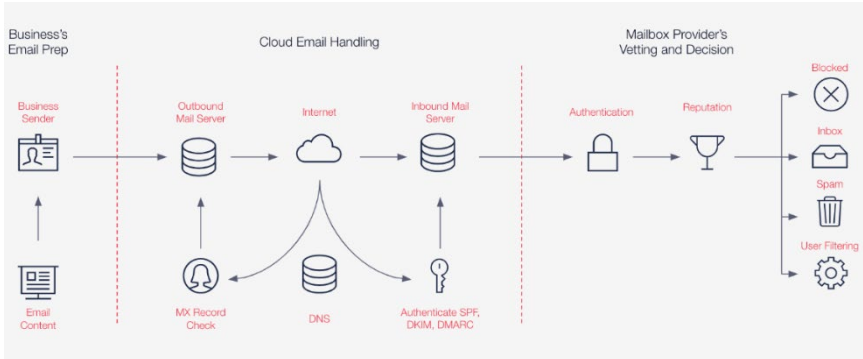
4.0 [Risk assessment](#)

5.0 Consult the DPO

Guidance: Submit your DPIA for consideration by the DPIA Forum. The process to follow is [here](#). Any recommendations from the DPOs team will be documented below and your DPIA will be returned to you. You should then record your response to each recommendation.

	<u>Recommendation</u>	Date and project stage	<u>Project Team Response</u>
	<p>Clarify the description of new service – we’re not clear about whether you are replacing an existing Sendgrid service with a new contract and supplier or whether are you amending the existing arrangements to add on additional processing? Consequently it’s not completely clear what’s currently in use, what’s being replaced / added to and what the new service is.</p>	<p>7 April 2022</p>	<p>I’ve added additional clarification into the description of the service in the DPIA: The service being reviewed/implemented is Twilio Sendgrid. Sendgrid is a cloud-based email service.</p> <p>Sendgrid is used to offload the creation and sending of emails, removing the need to run our own email infrastructure.</p> <p>Sendgrid is already used by the ICO website. In relation to the ICO website, the purpose of this DPIA is to ensure that a DPIA has been completed for its continued use.</p> <p>There are plans to use Sendgrid for ICE (see detail below).</p> <p><u>ICO website (existing)</u> The ICO website has used Sendgrid since 2018. It uses Sendgrid for sending emails comprising alerts such as success/failure messages, and for the sending the outputs of web forms as emails from the ICO website to ourselves, to our casework systems. There is <i>no proposed</i></p>

			<p><i>change</i> to the Sendgrid implementation for the ICO website.</p> <p><u>ICE (proposed)</u> There are plans for ICE (initially registration but with the likely extension for ICE 360) use Sendgrid to send system generated emails in the near future. ICE 360 would use Sendgrid to send communications to individual members of the public and individuals at organisations, for example casework correspondence and data breach information; the ICE Registrations system would use the service to send correspondence to data controllers (which may include sole traders) regarding their registration with the ICO, for example renewal reminders, direct debit notices, and notices of intent.</p>
	<p>Cyber Security Assessment - cyber colleagues flagged that they think Twilio Sendgrid is a new service and Cyber Security therefore need to be consulted about both the supplier assurance and the assessment of the product – so a supplier risk assessment and SOR are needed. Cyber Security assessed the Sendgrid Platform a long time ago and this doesn't compare to this new proposed service involving Twilio.</p>	<p>7 April 2022</p>	<p>Our use of Sendgrid for the website is existing, but I wanted to do an up to date DPIA for it given that any previous assessments were done a fairly long time ago, and given the proposed plans for ICE to use it. According to Wikipedia, Twilio announced plans to acquire Sendgrid in October 2018, which would have been around the time that Eduserv were implementing Sendgrid as part of the website move to the cloud. Twilio completed its acquisition in February 2019. This would explain the name change from Sendgrid to Twilio Sendgrid and perhaps why Cyber believe the service is different. However, despite the acquisition, the company has always been US-based and I believe the data flows have remained the same, so in relation to the website, the review should be regarded as 'existing'.</p>

			<p>Steve Rook and I had a conversation before I completed the draft DPIA and agreed that a supplier risk assessment should be completed. I'll follow up with the Cyber team about a SOR.</p> <p>05/07/2023 – A security opinion report for the service was concluded and the opinion is met: appropriate risk treatment has been performed to reduce the risk to acceptable levels.</p>
	<p>Explain end to end data flow – there was a general view that some elements need to be explained further for the group to fully understand the processing and provide recommendations e.g. Sendgrid data flow – what happens when ICO information makes it to SendGrid?</p>	<p>7 April 2022</p>	<p>I have added more information to the DPIA. See below for the additional information (please refer to the updated DPIA to see the additional information in context):</p> <p>In more detail ... 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.</p>  <p>The diagram illustrates the email flow process, divided into three main stages: Business's Email Prep, Cloud Email Handling, and Mailbox Provider's Vetting and Decision. 1. Business's Email Prep: An 'Email Content' icon points to a 'Business Sender' icon. 2. Cloud Email Handling: The flow goes from the 'Business Sender' to an 'Outbound Mail Server' (represented by a server rack icon), then through the 'Internet' (cloud icon) to an 'Inbound Mail Server' (server rack icon). Below this path, 'MX Record Check' and 'DNS' icons are shown with arrows pointing to the transition between the Outbound and Inbound Mail Servers. 3. Mailbox Provider's Vetting and Decision: The flow continues from the 'Inbound Mail Server' through 'Authentication' (lock icon) and 'Reputation' (trophy icon). 4. Final Outcomes: From the 'Reputation' stage, arrows point to four possible outcomes: 'Blocked' (circle with X), 'Inbox' (envelope icon), 'Spam' (trash can icon), and 'User Filtering' (gear icon). 5. Additional Checks: At the bottom, 'Authenticate SPF, DKIM, DMARC' (key icon) is shown with an arrow pointing to the 'Authentication' stage.</p>

			<p>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:</p> <ol style="list-style-type: none"> 1. The ICO application (ICE Registration or ICE360) makes an API call to the Sendgrid server. 2. Sendgrid verifies that the API username and API key used for authentication correspond to an active account 3. Sendgrid examines the incoming data to parse the message information, such as sender address, recipient, and message content. 4. The Sendgrid server takes the message information it gathered from our request and account settings (including analytics and TLS), and then repeats the process in Step 3 with the recipient's mail server. 5. The recipient's mail server checks the sending address, recipient address (to ensure they are a valid recipient), and message content. It checks the sending domain for any potential DNS issues, such as invalid DKIM and SPF signatures. 6. As long as there are no issues, the recipient's mail server will use the protocols POP3 or IMAP to retrieve the email and deliver the message to its intended recipient.
	<p>There is mention of a cookie pixel and tracking, message header and text of email. Can you provide</p>	<p>7 April 2022</p>	<p>Sendgrid provides the ability for customer to measure if emails have been opened and, if emails contain links, whether or not recipients clicked on links in the email. It also allows integration with</p>

	<p>more explanation about what the analytics are?</p>		<p>Google Analytics. It does this by adding a transparent, one-pixel image to the email if the customer has enabled tracking settings.</p> <p>ICO will set all tracking settings to 'Disabled'. I have added this to the actions, ie to ensure that all Tracking settings have been set to 'Disabled'.</p>
	<p>The existing dataflow and new data flow and use of sendgrid may be quite different but this isn't completely clear. It was commented that currently emails leave the ICO environment via O365. This change may see them being routed to Twilio in the US before they exit to the Internet and forward on to the recipient?</p>	<p>7 April 2022</p>	<p>See previous answers in relation to clarifying what's currently in use vs what is proposed. The data flow for the website has remained the same as it was when introduced in 2018. The DPIA includes that data may be processed by Twilio and its subprocessor Amazon Web Services, located in the US, for routing and transmission of emails worldwide.</p>
	<p>Necessity and proportionality – currently there is very limited information in 1.5. Further explanation is really required about what this approach offers versus current arrangements. Consideration needs to be given to why ICO needs to process data in the way that is being proposed. Why is it necessary to use a US based service here. Are there no UK based services, is the cost too high, do they provide a better</p>	<p>7 April 2022</p>	<p>I have added more information into the DPIA, see below:</p> <p>The processing is necessary in order for the ICO to exercise its official authority and carry out its public task, including providing a complaints service, providing a service for data controllers to register and pay, and communications about enforcement action.</p> <p>The use of an SMTP service is needed to offload the creation and sending of emails, removing the need to run our own email infrastructure.</p>

	<p>service etc? There just generally needs to be more explanation about why the planned approach is necessary.</p>		<p>ICE is currently exceeding the limits imposed by O365, which has a 10k daily limit on the number of emails that can be sent from a single address in a 24 hour period.</p> <p>Sendgrid was originally chosen for use by the ICO website in 2018 because it has strict anti-spam capabilities, and (unlike many other providers) offers sending from a dedicated IP address, both of which reduce the likelihood that the service is used by spammers and would result in ICO emails being refused or marked as spam or, at worst, blacklisted. Dedicated IP addresses additionally mean that ICO mail servers can easily be configured to recognise and route incoming emails from the service, mitigating the risk that our own email could be marked as spam or junk. Sendgrid also 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.</p> <p>For the above reasons Sendgrid is recommended by Microsoft for sending emails from Azure web apps.</p> <p>Sendgrid provides a simple SMTP relay option, as well as more advanced API integration that would support the ICO if we had future needs for sending emails from other applications.</p> <p>For ICE, an evaluation exercise was completed using G-Cloud but none of the listed suppliers met the ICO's technical requirements, in particular for a simple bulk email provider with an SMTP relay option (other products</p>
--	--	--	---

			evaluated were all geared towards sending marketing emails rather than transactional.)
	Overseas transfer – Mitigation for the overseas transfer risk should explain which of the appropriate safeguards referred to in UK GDPR is being put in place as this is the main mitigation to make the transfer lawful. As it stands without this in your mitigation the probability score should be 5. Implementing one of these safeguards will reduce the probability score (and expected risk score) to 1 so it is key. The Twilio privacy notice mentions both binding corporate rules and standard contractual clauses are used but you will likely need to ask legal to confirm what is actually in place for us.	7 April 2022	<p>I have increased the probability score to 5 for now. I'll await the advice from Legal about what mitigations will be in place for our use of the service.</p> <p>05/07/2023 – Contract, and Data Protection Addendum describe protections that are given for overseas transfers. Twilio state they rely on standard contractual clauses for the transfers.</p> <p>Transfer risk assessment completed and this concluded risk of harm to data subjects is low. Probability score for overseas transfer risk reduced to 2.</p>
	Some Cyber Security colleagues were unclear on whether they were being asked to assess the existing use of Sendgrid by the website, or the proposed use of Sendgrid by the ICE application. They advised	26 May 2022	See previous answers. The use of Sendgrid for each application had been split within the document, as well as the categories of data and controls put in place. However, as both applications will use the same Sendgrid account, covered by the same contract, many of the controls were common to both and both applications were essentially using the service to send data at OFFICIAL sensitive it had

	that the document should focus on only one use.		been agreed that the impact assessment for DP purposes was essentially the same. However, in response to the feedback, the document will now be split.
--	---	--	--

6.0 Integrate the outcomes back into your plans

Guidance: Identify who is responsible for integrating the DPIA outcomes. The outcomes include any expected mitigation you need to take as identified in your risk assessment and any further actions resulting from the DPOs recommendations.

Action	Date for completion	Responsibility for Action	Completed Date
Update Article 30 record of processing activities	28/06/2022	Information Management Service	28/06/2022 - SJ
Conduct Transfer Risk Assessment with regard to international transfers	Underway (unknown)	Commercial Legal	10/10/2022
Ensure analytics (opens and link tracking) settings are disabled	20/07/2023	Digital Architect	
Update Privacy Notices	ASAP	IM Service / Digital Architect	18/06/2022 -SJ

7.0 Expected residual risk and sign off

Guidance: Summarise the expected residual risk below. This is any remaining risk *after* you implement all of your mitigation measures and complete all actions.

It is never possible to remove all risk so this section shouldn't be omitted or blank. If the expected residual risk remains high (e.g. red on the traffic light scoring in the Appendix) then you will need to consult the ICO as the regulator by following the process used by external organisations.

Data is kept for longer than is necessary by data processor

Residual risk level: Green (1/1).

Contract makes the residual risk level very low, and impact would be very low.

Individual rights - Data processed without regard for statutory rights.

Residual risk level: Green (2/1).

Given that the contract commits Twilio to give reasonable assistance to customers responding to data subject requests in line with their rights, there is a residual likelihood that a request is received and responding to it requires assistance that the supplier assesses as beyond 'reasonable'. However, the impact is likely to be low as the ICO may be able to provide the data subject with a copy of the content of the email data from the website content management system (if within the retention period), or update their details (depending on the nature of the request).

Unauthorised access, destruction, loss, modification of data.

Residual risk level: Green (3/1).

If the content of an email was modified without authorisation, individuals receiving such an email from the ICO could experience significant inconveniences, including confusion and stress, likely to be overcome by the ICO needing to explain any situation and take appropriate action. Given the assurances provided by the contract, this should be considered very unlikely but some residual risk remains.

Data processor network / system / online portal not secure

Residual risk level: Green (3/1).

If the service was not appropriately secure, then unauthorised access could result in disclosure of email content that customers would expect to be private to the intended recipients. If this included sensitive material then this could cause significant consequences, which they should be able to overcome albeit but potentially with serious difficulties. Given the assurances provided by the contract, this should be considered very unlikely but some residual risk remains.

Data transferred overseas to a jurisdiction that does not adequately protect data subject rights

Residual risk level initially assessed at an impact of 1, and likelihood of 5. The likelihood is currently difficult to assess, given the uncertainty in the wake of the Schrems II judgement, therefore TLT have been engaged to complete a transfer risk assessment. This was completed and it was concluded that the processing was low-risk. The score was revised to 2.

7.1 [IAO sign off](#)

IAO (name and role)	Date	Project Stage

8.0 [Change history](#)

Guidance: To be completed by the person responsible for completing the DPIA and delivering the system, service or process)

Version	Date	Author	Change description
V0.1		Greer Schick	First draft
V0.2		Greer Schick	Updates from Emma Boyne re ICE processing
			Updates from conversations with Steven Johnston, Information Management and Compliance
V0.4	28 March 2022	Greer Schick	Submitted to DPIA Forum
V0.5	11 May 2022	Greer Schick	Updates from feedback from DPIA forum: description of service, more detail information flow, action to ensure opens and click settings are disabled, more information on necessity and proportionality, increase to likelihood risk rating re overseas transfers while we await legal advice and TRA.
V0.6	31 May 2022	Greer Schick	Updates from further feedback from DPIA forum to split document to cover only ICE use of Sendgrid (website use of Sendgrid covered in separate document).
V0.7	18/08/2022	Steven Johnston	Confirmation of completed action added to 6.0.
V0.8	12/07/2323	Greer Schick	Confirmation of completion of Transfer Risk assessment and update to 6.0.

Appendix 1: Risk Assessment Criteria

The following criteria are aligned with our corporate risk assessment criteria.

Impact

Impact is the consequence of a risk to the rights and freedoms of individuals being realised. Factors to consider include the financial harm or emotional distress that can be expected to occur.

Impact	Scoring criteria
Very low (1)	No discernible impact on individuals.

Low (2)	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc).
Medium (3)	Individuals may encounter significant inconveniences, which they will overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc)
High (4)	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc).
Very high (5)	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Probability

Probability is the likelihood of a risk to the rights and freedoms of individuals being realised. Factors to consider include the expected frequency of occurrence, and the motivation and capability of threat sources (eg does the threat require insider knowledge and/or significant technical resources to exploit any vulnerability?).

Probability	Scoring criteria
Very low (1)	0-5% - extremely unlikely or improbable For example, the risk has not occurred before or is not expected to occur within the next three years.
Low (2)	6-20% - low but not improbable For example, the risk is expected to occur once a year.
Medium (3)	21-50% - fairly likely to occur For example, the risk is expected to occur several times a year.
High (4)	51-80% - more likely to occur than not For example, the risk is expected to occur once a month.
Very high (5)	81-100% - almost certainly will occur For example, the risk is expected to occur once a week.

Risk level

Risk level is a function of impact and probability, and is represented by a RAG rating.

Probability \ Impact	Very low (1)	Low (2)	Medium (3)	High (4)	Very high (5)
Very high (5)	Amber (5)	Amber (10)	Red (15)	Red (20)	Red (25)
High (4)	Green (4)	Amber (8)	Amber (12)	Red (16)	Red (20)
Medium (3)	Green (3)	Amber (6)	Amber (9)	Amber (12)	Red (15)
Low (2)	Green (2)	Green (4)	Amber (6)	Amber (8)	Amber (10)
Very low (1)	Green (1)	Green (2)	Green (3)	Green (4)	Amber (5)

Risk acceptance criteria

These criteria are guidelines only, and any risk treatment decisions should be made on a case-by-case basis. For example, it may be prudent to reduce a low risk because of legal and regulatory requirements.

Risk level	Acceptance criteria
Low (Green)	Within this range risks can be routinely accepted.
Medium (Amber)	Within this range risks can occasionally be accepted but shall be kept under regular review.
High (Red)	Within this range risks shall not be accepted and immediate action is required to reduce, avoid or transfer the risk.

Appendix 2: example risks to data subjects

Guidance: The following are examples of common risks associated with the processing of personal data to assist with your risk assessment. Not all of them will apply to your processing and the list is not exhaustive – you should consider specific risks that are relevant to your plans.

- Data is processed for unspecified / unlawful purposes/ not within expectations of data subjects
- Excessive data is processed
- Data is not kept up to date

- Data is kept for longer than is necessary by us
- Data is kept for longer than is necessary by data processor
- Data processed in contravention of data subject rights
- Data subjects unable to exercise their rights
- Data stolen or modified in transit
- Data stolen or modified at rest in our premises
- Data stolen or modified at rest in data processor premises
- Data transferred overseas to a jurisdiction that does not adequately protect data subject rights
- Re-identification of pseudonymised data by data processor or third party
- Unauthorised destruction or loss of data
- Data processor network / system / online portal not secure
- Data processor fails to process data in accordance with our instructions
- Personal data of children processed without appropriate safeguards / parental authority
- Consent of data subject not freely given (for example employer / employee processing)
- The data subject is particularly vulnerable (elderly or disabled) or is there a potential imbalance of power between the individual and the controller (employee/employer)
- Source of data poses risks re accuracy (obtained from a unverified or old list)
- Risk to accuracy of data due to matching / combining data from different sources
- Use of new technology, e.g. fingerprinting, face recognition
- Monitoring or recording individuals
- Using profiling according to characteristics or behavior
- Non-compliance with DP principles

9.0 Template Change History (for Information Management Service only)

Version	Date	Author	Change description
v0.1	01/06/2020	Steven Johnston	First draft
v1.0	07/10/2020	Steven Johnston	First release
v1.1	07/01/2021	Iman Elmehdawy	Amendment to guidance note page 2.

v1.2	18/03/2021	Helen Ward	Addition of Privacy by design at the ICO (pages 2 and 3)
v1.3	24/06/2021	Steven Johnston	Section 3.0 Q13 amended. Removed request for link to security assessment.