

Records of Processing. Data Protection Analysis.

Report-URI Ltd.

22 Shireburn Avenue
Clitheroe
BB7 2PN

Version 1.4R
March 2021

1 Contents

Table of Contents

1	Contents	2
2	Version Control	3
3	Terms	4
4	Purpose	4
5	Introduction	4
6	Records of Processing	5
6.1	Free Users	5
6.2	Paying Users	6
6.3	Enterprise Users	7
7	Sales and Marketing Activities	8
8	Technical Support	8
9	Error Logging	8
10	Systems and Third-party Processors	8
11	Summary of Personal Data Processing	9
11.1	User Email Address	9
11.2	User Password	10
11.3	User Payment Data	10
11.4	Miscellaneous Contact Information	11
12	Data Minimisation and Privacy by Design and Default	11
13	Use of Cookies	12
13.1	Cloudflare Cookies	12
13.2	Stripe Cookies	12
14	Security	12
14.1	Cyber Essentials	12
14.2	Penetration Test	13
14.3	PCI DSS Compliance	13
15	Is a DPIA Required?	13
16	Should a DPO be Appointed?	13
17	Should an EEA Representative be Appointed?	14
18	Report-URI as a Processor	14
18.1	Are Report-URI's Customers Subject to UK or EU GDPR?	14
18.2	Do Telemetry Reports Contain Personal Data?	14
18.3	Summary	16
18.4	Identification of Report-URI as a Processor by a Report-URI Customer	16
18.5	Telemetry Information: Privacy by Design	18

2 Version Control

Version	Date	Changes	Status
1v0	18 Dec 20	Descriptions of processing	Draft
1v1	06 Jan 21	Feedback from Scott, completion of tbc	Draft
1v2	28 Jan 21	Minor edits	Draft
1v3	01 Mar 21	Updates to reflect changes in privacy policy and legal analysis document	Draft
1v4	05 Mar 21	Added screenshots	Final

3 Terms

Terms used in this document are as defined in Article 4 of the EU General Data Protection Regulation (GDPR) unless otherwise noted.

4 Purpose

This document records the processing of personal data undertaken by Report-URI. It fulfils the requirement of Article 30, and in respect of Article 35 an analysis of whether a DPIA is necessary.

Report-URI is a Controller for a limited amount of personal data and may also act as a Processor.

Report-URI is registered with the ICO, registration number ZA860641.

5 Introduction

Report-URI provides a SaaS solution that enables organisations to collect error and telemetry information about how their website is received by their customer's browsers. Additionally, it also will allow the collection of telemetry about their email security configuration from recipient email servers.

Many internet protocols now allow for an endpoint (whether that is a consumer browser or email server) that detects an error or policy violation to send a report to the owner of the webpage or the originator of the email. This is typically specified in the REPORT-URI parameter of a directive – hence the service's name.

Report-URI allows a user to create an account, once that account has been created the user can then direct such error reports to the Report-URI service. The service intelligently interprets, parses, consolidates and normalises the telemetry reports. The service then allows the user to query the normalised telemetry data received in the form of on-screen reports.

The service is available free of charge but requires payment once the number of telemetry reports exceeds a monthly threshold.

Payment for the service is by monthly payment card billing (account on file).

Some larger 'enterprise' customers can additionally pay by bank transfer in receipt of an invoice.

For clarity, these three classes of customer will be described in this document as:

- Free Users
- Paying Users
- Enterprise Users

6 Records of Processing

6.1 Free Users

To create an account a user needs to provide an email address and password. These are stored in Report-URI's core systems.

The email address is used as the unique identifier for the user to login.

The password is salted with 128 bits of entropy and hashed using 1024 rounds of Bcrypt.

A unique internal user ID is also generated for the account.

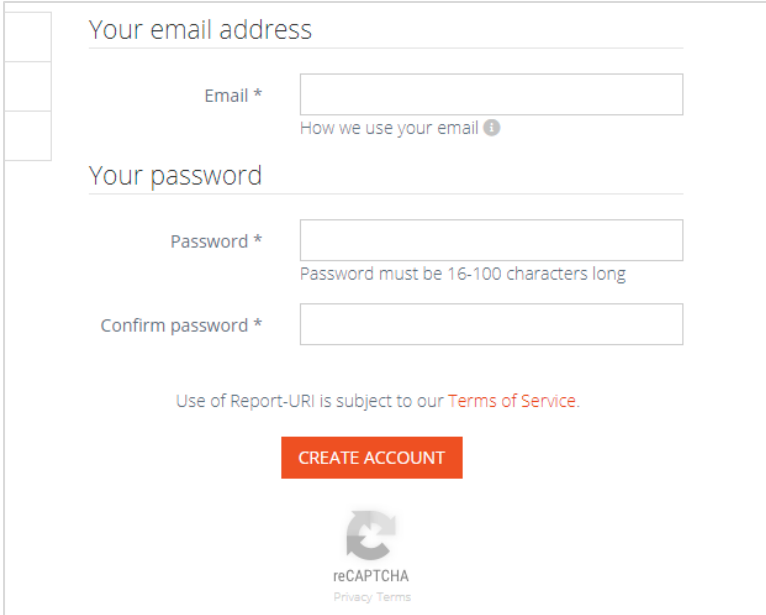
The user may also select a unique sub-domain prefix (e.g. mysubdomian.report-uri.com).

The use of the email address, password, internal user ID and (where requested) sub-domain are necessary for the operation of the service.

The email address is verified: on registration the email address entered is sent a validation email which contains a unique link. To complete registration this unique link must be clicked which confirms that the user is in control of the email address specified.

No other personal data is processed in respect of Free Users.

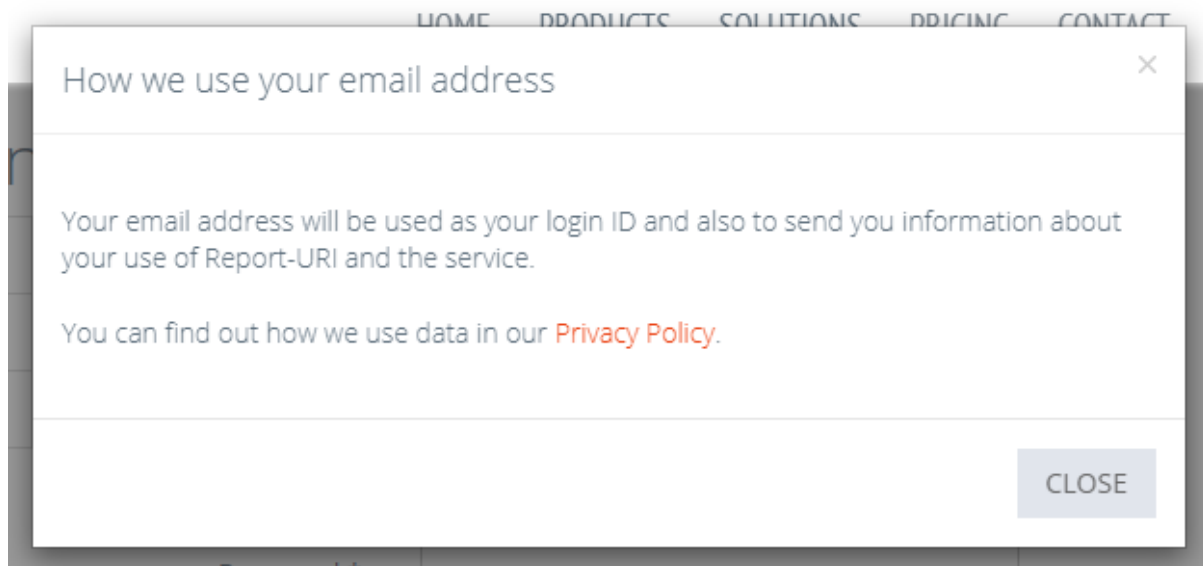
An icon and a link "*How we use your email*" is placed directly under the field where the user enters their email address on the registration page.



The screenshot shows a registration form with the following elements:

- Your email address**: A text input field labeled "Email *". Below the field is a link "How we use your email" with an information icon.
- Your password**: A text input field labeled "Password *". Below the field is a note "Password must be 16-100 characters long".
- Confirm password ***: A second text input field for password confirmation.
- Terms of Service**: A line of text stating "Use of Report-URI is subject to our [Terms of Service](#)."
- CREATE ACCOUNT**: A prominent orange button.
- reCAPTCHA**: A reCAPTCHA logo and the text "reCAPTCHA Privacy Terms" at the bottom.

The user can click on this link and the resulting pop-up provides contextual information about the use of the user's email address and a link to the full privacy policy.



6.2 Paying Users

Once a user decides to add a payment card to their account (typically to upgrade from a Free User to Paying User) the following information is collected:

- A company or person name
- The country of residence
- The billing address, city, and postcode that the payment card is registered to
- An optional EU VAT ID
- The Primary Account Number (PAN), expiration date and verification code of the payment card.

The data is transmitted from the user's computer directly to Stripe, the third-party service provider used to manage payment card billing.

Stripe returns a reference to Report-URI that is associated with the user's account.

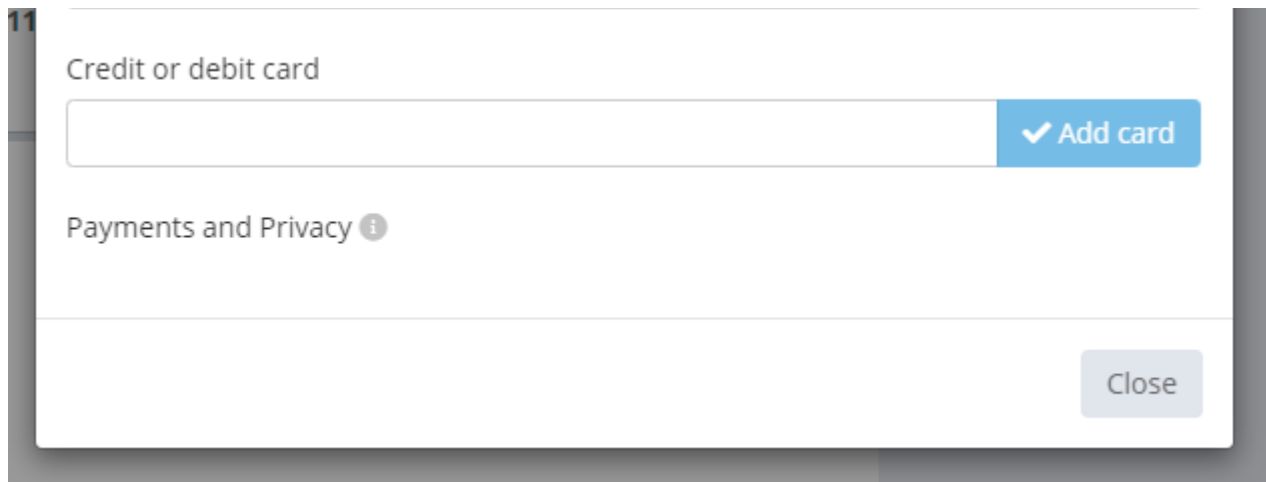
This reference is used by Report-URI to change recurring billing instructions.

The collection and processing of all this data is necessary to enable payment card billing.

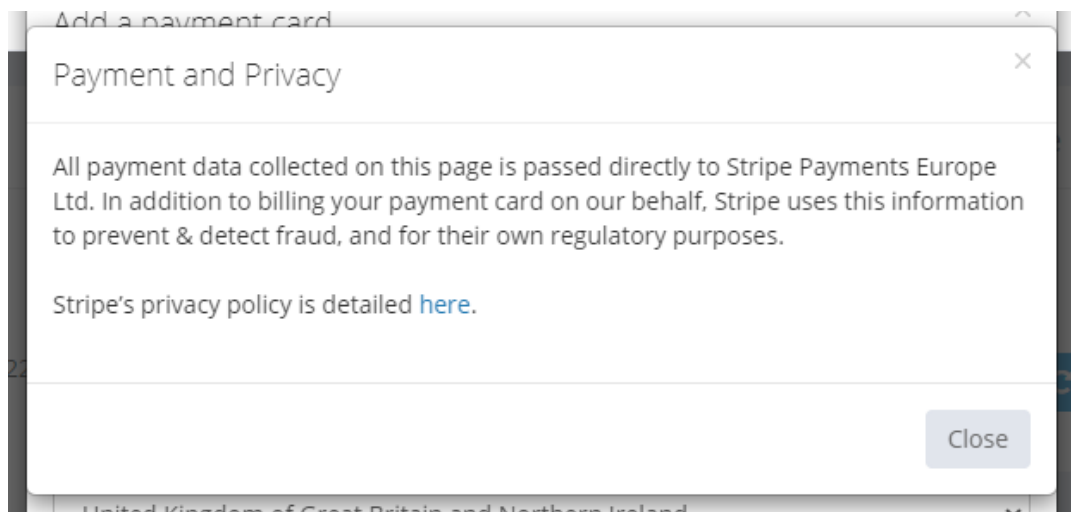
Stripe is acting as a Processor for Report-URI when it is asked to collect a payment.

Stripe also acts as a Controller in its own right for the purpose of detecting fraud, and its legal and regulatory obligations.

On the page where the payment data is collected, a link and an icon indicates that there is more information available about the processing of payment data.



When this link is clicked the following pop-up is displayed.



6.3 Enterprise Users

Information necessary for sending invoices and collecting payments is obtained directly from customers. This generally includes data relating to one or more individuals at each enterprise user. The data collected includes:

- Names
- Job Titles
- Email address
- Office address
- Telephone numbers

This data is usually collected via email and is a sub-set of data is manually transcribed into Sage Accounts, a cloud-based third-party service provider that provides accounting and invoicing services.

7 Sales and Marketing Activities

No systems are used in respect of sales and marketing activities. Enquiries are generally dealt with via email.

8 Technical Support

Support is provided to customers via email. There is no customer-facing ticketing system. An internal system is used to track work and fixes, if a particular bug is related to a user, this is referenced by the internal user ID rather than the user's email address.

9 Error Logging

The system creates automatic logs of error activity. If this is associated with a particular user action, then the internal user ID is stored.

10 Systems and Third-party Processors

The core Report-URI systems run on cloud services.

Name	Services	Location
Cloudflare	Edge computing, CDN, WAF	US+ others
Digital Ocean	Core application processing on Report-URI administered systems hosted on Digital Ocean hypervisor plane	US
Fastmail	Email services	AU
Microsoft Azure	Core application storage Database services	US
Sendgrid	Core application Email sending and receipt (SMTP servers)	US
Sage	Accounting SaaS	UK
Stripe	Payment Services	Dublin, EU

Compliant service contracts are in place with all third-party processors. Where this involves transfers outside the UK or EEA, SCCs are in place.

Although the position of SCCs is in doubt following the Schrems II decision, the data transferred outside the EEA (practically email address and password hash) would not be of interest to nation state entities and even if accessed would pose extremely limited risks to the fundamental rights and freedoms of Report-URI's customers.

11 Summary of Personal Data Processing

11.1 User Email Address

Source	Entered by user
Reason (s) for processing	Used as the unique identifier to allow login Used to send emails about account activity, billing etc Used to send updates about the service or reporting protocols
Legal basis for processing	The performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
Accuracy	Verified by user clicking on link in email sent to the address
Retention	Retailed as long as account is in use
Deletion by user	A user can delete their own account, this will delete this data
Deletion by report URI	This functionality exists but is currently disabled
Systems processing	Core application Cloudflare Sendgrid
Systems storing	Core application (Azure) Stripe (if paying) Sage (if enterprise invoice contact)

11.2 User Password

Source	User entered – hashed value stored
Reason (s) for processing	To allow authentication of a user
Legal basis for processing	The performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
Accuracy	Validated by user being able to login
Retention	Retained as long as account is in use
Deletion by user	A user can delete their own account, this will delete this data
Deletion by Report-URI	This functionality exists but is currently disabled
Systems processing	Core application
Systems storing	Core application stores hash only

11.3 User Payment Data

Source	User entered. <ul style="list-style-type: none"> • Entity or person name • Billing address • PAN, Expiration Date, CVC2
Reason (s) for processing	To enable billing
Legal basis for processing	The performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract
Accuracy	Validated by Stripe
Retention	As long as billing is needed
Deletion by user	When user deletes account or a user deletes their card form the account.
Deletion by Report-URI	Manual process to login to Stripe and delete.
Systems processing	Stripe
Systems storing	Stripe

11.4 Miscellaneous Contact Information

Source	User provided (typically emails)
Reason (s) for processing	The performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
Accuracy	User provided
Retention	As long is necessary to deal with matters
Deletion by user	Not available
Deletion by Report-URI	Depends on context
Systems processing	Local email clients, Fastmail
Systems storing	Local email clients, Fastmail

12 Data Minimisation and Privacy by Design and Default

As can be seen from the above description, care has been taken to only collect and process the minimum data needed to provide the service to the users.

There is no secondary use of the data collected by Report-URI.

Stripe makes secondary use of the payment data passed to it for fraud prevention and regulatory purposes, but it does this in the context of a Controller in its own right. Since GDPR became effective this approach that payment processors and acquirers make such secondary use of data is standard across the industry.

13 Use of Cookies

The following cookies are set:

Type	Cookie	Purpose
1 st	__Host-report_uri_csrf	CSRF prevention
1 st	__Host-report_uri_sess	Session cookie
1 st	__cf_bm	Cloudflare Bot Management
1 st	__cfduid	Cloudflare client identifier
1 st	__stripe_mid	Fraud prevention and detection
1 st	__stripe_sid	Fraud prevention and detection
1 st	_nss	Nette SameSite, used in admin panel to protect against CSRF
1 st	__Secure-hideSeries-<report type>	where <report type> currently csp only, but the code is generic enough to support all report types. Set by JavaScript.
1 st	sidebar_closed	set when the user closes the sidebar
3 rd	m (m.stripe.com)	Fraud prevention and detection

13.1 Cloudflare Cookies

Cloudflare Cookies are detailed at <https://support.cloudflare.com/hc/en-us/articles/200170156-Understanding-the-Cloudflare-Cookies>

13.2 Stripe Cookies

Stripe Cookies are detailed at <https://stripe.com/cookies-policy/legal>

14 Security

Report-URI was established by Scott Helme, an experienced information security professional who was later joined by Troy Hunt and Michal Špaček. All three principals regularly teach information security.

It should be remembered that from a data protection perspective this level of security is to protect the only personal data processed by Report-URI which is the username and password.

14.1 Cyber Essentials

Report-URI was assessed against and achieved the Cyber Essentials certification in January 2019¹ this has been renewed annually and the current certification expires in July 2022.

¹ <https://scotthelme.co.uk/getting-cyber-essentials/>

14.2 Penetration Test

In December 2020 Report-URI commissioned an external “white box” penetration test from PenTest Limited. The results of this have been published in full along with an analysis of the vulnerabilities found and how they were rectified.²

14.3 PCI DSS Compliance

The payment data is collected in a IFRAME served directly from and returned to Stripe. This meets the eligibility criteria of PCI DSS SAQ A³ which is completed annually and provided to Report-URI’s acquiring bank.

The use of an IFRAME protects against e-commerce skimming (aka Magecart) attacks and means that Report-URI’s systems do not store, process, or transmit payment card data.

Administrative access to Stripe’s customer portal where the payment information entered by the paying customer can be viewed (masked PAN only) is protected by two-factor authentication.

15 Is a DPIA Required?

Article 35 of the EU GDPR requires an organisation to undertake a Data Protection Impact Assessment (DPIA) where processing is “likely to result in a high risk to the rights and freedoms of natural persons”.

The processing of email addresses – which are typically corporate email addresses and standard payment card information is unlikely to result in a high risk, and accordingly a DPIA is not required for Report-URI’s current processing.

Any new processing of personal data will be evaluated before processing commences to determine whether a DPIA is required.

16 Should a DPO be Appointed?

Article 37 of the EU GDPR defines three criteria by which an entity must appoint a Data Protection Officer (DPO).

The activities of report-URI do not meet any of these criteria:

- Report-URI is not a public body or authority.
- Report-URI does not “require regular and systematic monitoring of data subjects on a large scale”.
- Report-URI does not conduct “processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10”.

Accordingly Report-URI is not required to appoint a DPO.

² <https://scotthelme.co.uk/report-uri-penetration-test-2020/>

³ https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2_1-SAQ-A.pdf

17 Should an EEA Representative be Appointed?

Report-URI is essentially a business-to-business service, used by organisations, although there are some individual consumer users these do not represent the target market. As such neither article 3(2)(a) or 3(2)(b) of the EU GDPR apply.

Even if it were held that Report-URI does come into scope of the EU GDPR, the derogation provided by Article 27(2) would apply. The processing of personal data by Report-URI is occasional and does not include the processing of any special category personal data. A breach of confidentiality of the personal data processed by Report-URI would be unlikely to result in a risk to the rights and freedoms of natural persons.

Report-URI does not need to appoint a representative in the EU.

18 Report-URI as a Processor

Report-URI receives telemetry reports from the browsers and email gateways of its Customers' customers. i.e. the reports come directly from the end user customers / clients of people visiting Report-URI's Customers' websites.

If a Report-URI Customer is subject to UK or EU GDPR, and the telemetry report contains personal data as defined by the GDPR, then Report-URI will be acting as a Processor for its Customers and therefore Article 28 will be applicable to Report-URI.

18.1 Are Report-URI's Customers Subject to UK or EU GDPR?

Some are. Although a separate record is not maintained of whether a Report-URI Customer is subject to GDPR, a quick look at the client list shows many UK and EU-based companies.

18.2 Do Telemetry Reports Contain Personal Data?

There is not a clear answer to this question. Data that is included in telemetry reports which may be classified as Personal Data include:

18.2.1 IP Address

The IP address of the reporter's system is received with a telemetry report. This information may or may not be personal data depending on the activities of Report-URI's Customer – i.e., whether the IP address is able to be related to an individual identifiable by the Customer.

However, although the IP address is received at the Cloudflare Edge node nearest to the reporting consumer browser, it is immediately discarded at Cloudflare and it is not forwarded to the core Report-URI system.

Technically, for some of Report-URI's Customers the IP address may be able to be related to an individual, however because the data is not, and cannot, be stored by Report-URI, it is impossible that this can practically occur.

18.2.2 HTTP-Referrer

The HTTP-Referrer (i.e. the previous page URI that the user was visiting and where they clicked the link to the URI that generated the telemetry report) may be included in a telemetry report. This information may or may not be personal data depending on the configuration of the referring page, and therefore Report-URI's Customer may be able to identify an individual from the combination of HTTP-Referrer, Reporting URI and timestamp.

The default behaviour is that the HTTP-Referrer is discarded by Report-URI before the telemetry report is stored. However, this can be overridden by the Customer.

18.2.3 Document URI

Depending on the format of the Document URI it may contain personal data, e.g.

```
www.customer.com/profile/John_Doe/
```

This information would be retained by Report-URI and appear in reports.

18.2.4 Query String

Personal data may appear in query string variables received as part of a URI, e.g.

```
www.customer.com/editprofile?userID=12345&name=JohnDoe
```

The default behaviour is that all query string variables are discarded by Report-URI before the telemetry report is stored. However, this can be overridden by the Customer.

18.2.5 URI Fragment

A URI Fragment may relate to an identified or identifiable person, e.g.

```
www.customer.com/editprofile#JohnDoe-12345
```

The default behaviour is that all fragments are discarded by Report-URI before the telemetry report is stored. However, this can be overridden by the Customer.

18.2.6 Summary of Potential Personal Data Processed

Element	Received	Stored	Retained	Downloadable
IP Address	No*	No	-	-
HTTP Referrer	Yes	Default: No Configurable by Customer	90 days	No
URI	Yes	Yes	90 days	No
Query String	Yes	Default: No Configurable by Customer	90 days	No
Fragments	Yes	Default: No Configurable by Customer	90 days	No

* IP address is received by Cloudflare (a sub-processor of Report-URI) along with the telemetry report; however the IP address is not forwarded to the Report-URI core application and is discarded within the processing that occurs Cloudflare.

18.3 Summary

Report-URI may act as a Processor of the personal data of a Customer's customer. It is unable to determine this itself as this depends on the configuration of the Customer's website. Therefore, Customers must formally notify Report-URI if this is the case.

Report-URI has produced a document describing the circumstances in which it may act as a Processor to help Customers make this determination.

18.4 Identification of Report-URI as a Processor by a Report-URI Customer

An option is available in the account settings page where a user can nominate Report-URI as a Processor by amending the standard Terms of Service to incorporate a Data Processing Agreement (DPA).

18.4.1 Free Users

This option in the settings menu can be accessed by a Free User, however they are invited to upgrade to a paid-for account to be able to incorporate the DPA as an amendment to the Terms of Service. This ensures that there is a formal relationship between the Controller and Report-URI in accordance with Article 28(3).

Controller-Processor Relationship

If you have determined that:

- a) the telemetry and violation reports contain the personal data of your website visitors and customers for which you are a Controller, and
- b) as a Controller you are subject to UK or EU GDPR, You may want Report-URI to act as your Processor in accordance with Article 28 of the EU GDPR which will be subject to our Data Processing Agreement.

If you wish to incorporate our Data Processing Agreement as an amendment to the Report URI [Terms of Service](#), please [upgrade](#) to any paid plan.

[Information about Teams](#) ⓘ

18.4.2 Paying and Enterprise Users

When a Paying or Enterprise User accesses the option in the settings menu, they can incorporate the DPA into the terms of service.

Controller-Processor Relationship

If you have determined that:

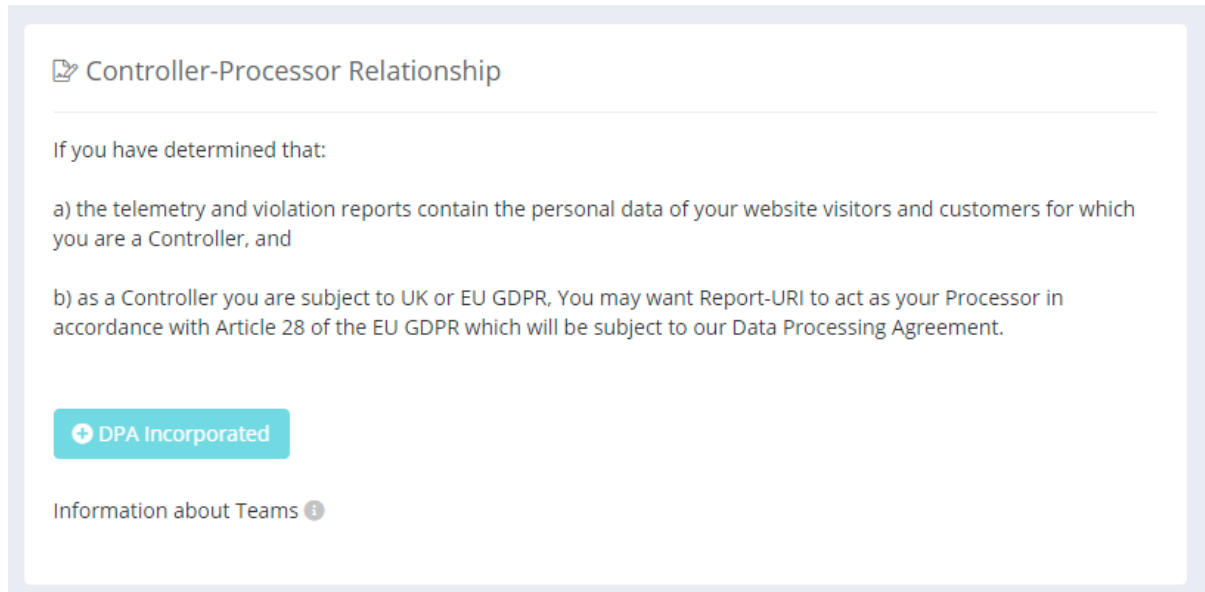
- a) the telemetry and violation reports contain the personal data of your website visitors and customers for which you are a Controller, and
- b) as a Controller you are subject to UK or EU GDPR, You may want Report-URI to act as your Processor in accordance with Article 28 of the EU GDPR which will be subject to our Data Processing Agreement.

If you wish to incorporate our Data Processing Agreement as an amendment to the Report URI [Terms of Service](#), please do so here:

[+ Incorporate DPA](#)

[Information about Teams](#) ⓘ

The date and time this option was selected is recorded, and the button changes to show that the User has enabled this option.



18.5 Telemetry Information: Privacy by Design

When designing the internet standards that allow for telemetry and error reporting, privacy and data protection were a significant concern. Information about the privacy implications of telemetry and violation reporting is available in the following documents.

Document	Location
General W3C Reporting API	https://www.w3.org/TR/reporting/#privacy
Content Security Policy (CSP)	https://www.w3.org/TR/CSP3/#security-considerations
Network Error Logging (NEL)	https://www.w3.org/TR/network-error-logging/#privacy-considerations
Domain-based Message Authentication, Reporting, and Conformance (DMARC)*	https://tools.ietf.org/html/rfc7489#section-9
Transport Layer Security for Simple Mail Transport Protocol (SMTP over TLS)	https://tools.ietf.org/html/rfc8460#section-8
Certificate Transparency (CT)	https://tools.ietf.org/html/rfc6962

* The forensic reporting option in DMARC (ruf) will expose the private information contained in an email. Report-URI does not support this option.