Catapult.

EU GDPR
Compliance Document

Contents.

GDPR Overview

Our compliance with the European Union General Data Protection Regulation.

What is GDPR?

The General Data Protection Regulation is an over arching data protection law that applies to all European Union residents from 25th May 2018. It deals with concerns around personal data that can directly or indirectly identify a person residing in the EU.

Identify

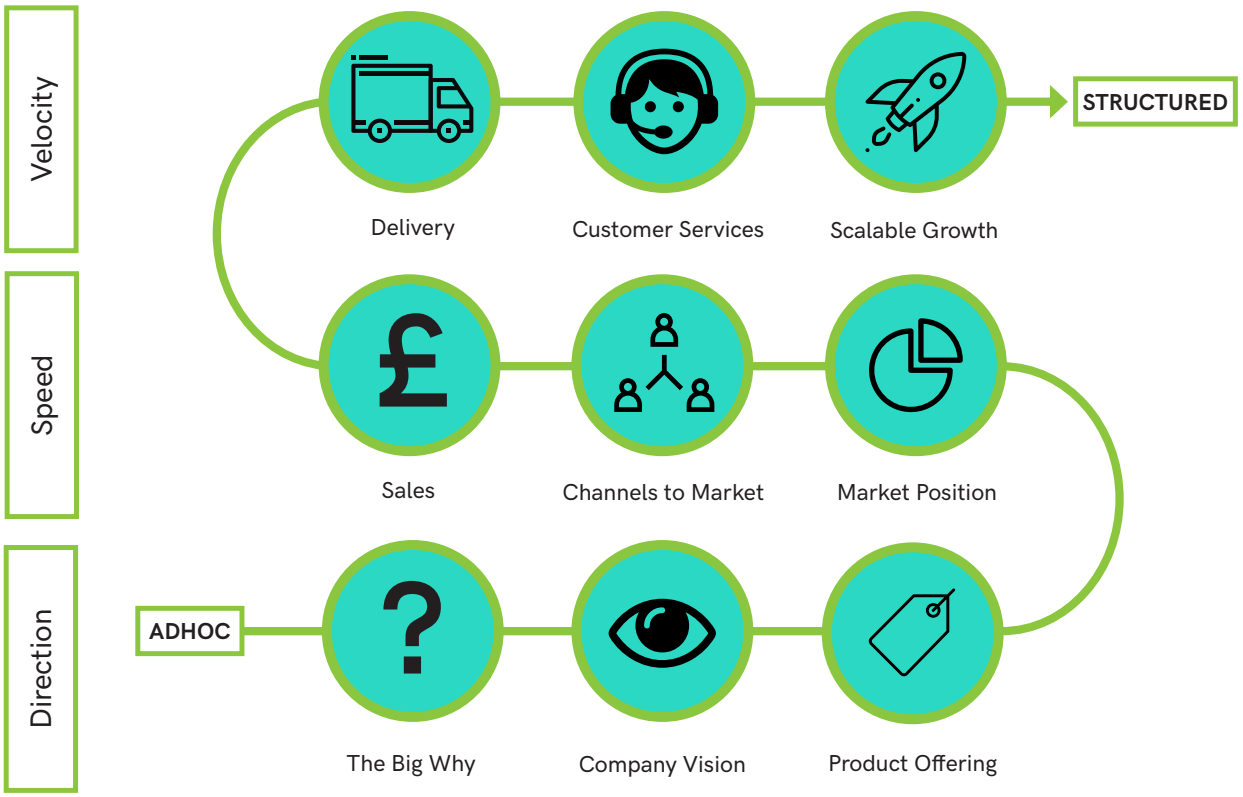
Collection, processing, storage and transfer

How Catapult identifies the data within the company.

About Catapult

Catapult works with ambitious business owners to choose life. We work with business owners to shift their perspective so that they can see that they can design a business around the type of life that they want to live, rather than living life that is dictated by the business needs.

We do this through our 9-step consultancy model which breaks down each of the key business areas.



Catapult.

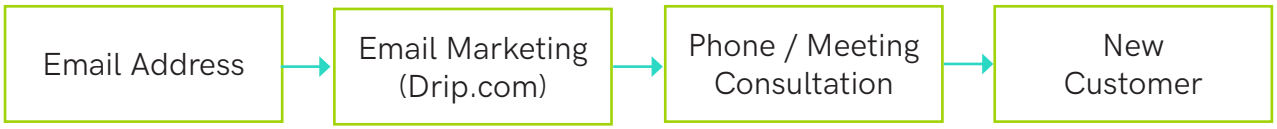
Each of the steps are further broken down into:

1. Concept
2. Strategy
3. Execution

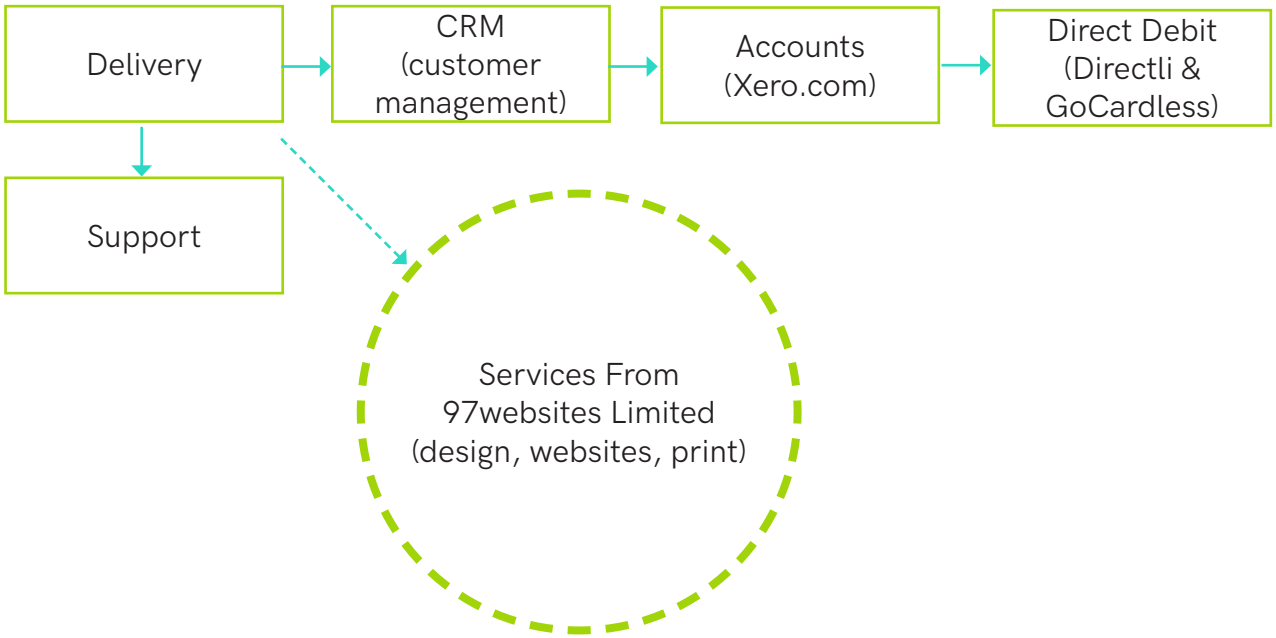
Our Systems

Catapult collects information from the following information systems / business areas. We do not collect any data that GDPR defines as "Special".

Channel To Market & Sales Process



Delivery & Customer Services



Sales Process Data

Email Address - is collected as part of our sales process. The email address is stored in drip.com an email marketing SAAS solution.

First Name - The first name is also collected for email marketing.

Phone consultation - When a customer would like to find further information about our services we will book a phone consultation. At this point we will collect a phone number.

Customer Services

Should a partner want to establish an account with us then we will add their information into our CRM system.

1. First Name
2. Second Name
3. Company Name
4. Email Address
5. Address inc Post Code
6. Phone Number
7. Notes and documents collected during consultation (bound by a non-disclosure agreement)

Accounts Data

We are a private limited company in the UK and we have an obligation to hold accounts. We use xero.com to manage our accounts.

XERO TRANSFER COMPLIANCE:

Safeguards for data stored in the US
We use top-tier, third-party services located in the US to host our online and mobile services. This means that personal information is transferred to servers in the US. To satisfy the requirements relating to the transfer of data from the EU to the US, we have agreements in place with each of our hosting providers that use European Commission model contract clauses. - Xero.com

Directli.co.uk & Gocardless.com

We use gocardless.com to collect payment via direct debit.

We use directli.co.uk to integrate our xero.com accounts system with gocardless.com.

We do not hold or receive any financial data such as bank account numbers or sort code numbers. These are managed by gocardless and directli, they comply with all financial regulations and GDPR.

GoCardless is based in the UK.

Directli is based in the UK.

Personal Data Inventory

WHY	WHO	WHAT			WHEN			WHERE
		Type	Source	Legal Basis	Originally	Retention Period	Determined by:	
DIRECT MARKETING	Prospect	Email Address First Name Phone Number	Partner	Consent	Website form, email or from phone call	Consent withdrawn	Business process	Email marketing drip.com
ACTIVE CUSTOMER	Partner	First Name Second Name Company Name Email Address Address & Post Code Phone Number	Partner	Performance of Contract	From direct marketing, or onboarding of customer	Consent withdrawn or closing of account These records may be kept if needed for accounts	Accounting Laws Tax Laws	CRM xero.com directli.co.uk gocardless.com
BUSINESS ADMIN	Partner	First Name Second Name Company Name Email Address Address & Post Code Phone Number Financial Data	Partner	UK Law	Supplied during the onboarding of the partner	Determined by UK law on how long to hold accounting information for taxation and legal compliance	UK Law	xero.com gocardless.com directli.co.uk
SUPPORT	Partner	First Name Second Name Email Address Email Content	Partner	Performance of Contract	Supplied to us when a support ticket is raised	12 months or if consent is withdrawn	Business process	Email ticketing system

Manage

Accountability & Management

In this section we look at who is responsible and how we manage data within the business.

Data Protection Policy

1. Introduction

1.1 We are committed to safeguarding the privacy of our website visitors and service users.
1.2 This policy applies where we are acting as a data controller with respect to the personal data of our website visitors and service users; in other words, where we determine the purposes and means of the processing of that personal data.
1.3 By using our website and agreeing to this policy, you consent to our use of cookies in accordance with the terms of this policy.
1.4 In this policy, "we", "us" and "our" refer to Catapult Training Limited t/a Catapult

2. Credit

2.1 This document was created using a template from SEQ Legal (https://seqlegal.com). You must retain the above credit. Use of this document without the credit is an infringement of copyright. However, you can purchase from us an equivalent document that does not include the credit.

3. How we use your personal data

3.1 In this Section 3 we have set out:
(a) the general categories of personal data that we may process;
(b) in the case of personal data that we did not obtain directly from you, the source and specific categories of that data;
(c) the purposes for which we may process personal data; and
(d) the legal bases of the processing.
3.2 We may process data about your use of our website and services ("usage data"). The usage data may include your IP address, geographical location, browser type and version, operating system, referral source, length of visit, page views and website navigation paths, as well as information about the timing, frequency and pattern of your service use. The source of the usage data is our analytics tracking system. This usage data may be processed for the purposes of analysing the use of the website and services. The legal basis for this processing is our legitimate interests, namely monitoring and improving our website and services.

3.3 We may process your account data ("account data"). The account data may include your name and email address. The source of the account data is you or your employer. The account data may be processed for the purposes of operating our website, providing our services, ensuring the security of our website and services, maintaining back-ups of our databases and communicating with you. The legal basis for this processing is the performance of a contract between you and us and/or taking steps, at your request, to enter into such a contract.
3.4 We may process your information included in your personal profile on our website ("profile data"). The profile data may include your name, address, telephone number, email address, profile pictures, gender, date of birth, relationship status, interests and hobbies, educational details and employment details. The profile data may be processed for the purposes of enabling and monitoring your use of our website and services. The legal basis for this processing is consent.
3.5 We may process your personal data that are provided in the course of the use of our services ("service data"). The service data may be processed for the purposes of operating our website, providing our services, ensuring the security of our website and services, maintaining back-ups of our databases and communicating with you. The legal basis for this processing is consent.
3.6 We may process information that you post for publication on our website or through our services ("publication data"). The publication data may be processed for the purposes of enabling such publication and administering our website and services. The legal basis for this processing is consent.
3.7 We may process information contained in any enquiry you submit to us regarding goods and/or services ("enquiry data"). The enquiry data may be processed for the purposes of offering, marketing and selling relevant goods and/or services to you. The legal basis for this processing is consent.
3.8 We may process information relating to transactions, including purchases of goods and services, that you enter into with us and/or through our website ("transaction data"). The transaction data may include your contact details, your card details and the transaction details. The transaction data may be processed for the purpose of supplying the purchased goods and services and keeping proper records of those transactions. The legal basis for this processing is the performance of a contract between you and us and/or taking steps, at your request, to enter into such a contract and our legitimate interests, namely our interest in the proper administration of our website and business.
3.9 We may process information that you provide to us for the purpose of subscribing to our email notifications and/or newsletters ("notification data"). The notification data may be processed for the purposes of sending you the relevant notifications and/or newsletters. The legal basis for this processing is consent.
3.10 We may process information contained in or relating to any communication that you send to us ("correspondence data"). The correspondence data may include the communication content and metadata associated with the communication. Our website will generate the metadata associated with communications made using the website contact forms. The correspondence data may be processed for the purposes of communicating with you and record-keeping. The legal basis for this processing is our legitimate interests, namely the proper administration of our website and business and communications with users.
3.11 We may process any of your personal data identified in this policy where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure. The legal basis for this processing is our legitimate interests, namely the protection and assertion of our legal rights, your legal rights and the legal rights of others.
3.12 We may process any of your personal data identified in this policy where necessary for the purposes of obtaining or maintaining insurance coverage, managing risks, or obtaining professional advice. The legal basis for this processing is our legitimate interests, namely the proper protection of our business against risks.

3.13 In addition to the specific purposes for which we may process your personal data set out in this Section 3, we may also process any of your personal data where such processing is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.
3.14 Please do not supply any other person's personal data to us, unless we prompt you to do so.

4. Providing your personal data to others
4.1 We may disclose your personal data to any member of our group of companies (this means our subsidiaries, our ultimate holding company and all its subsidiaries) insofar as reasonably necessary for the purposes, and on the legal bases, set out in this policy.
4.2 We may disclose your personal data to our insurers and/or professional advisers insofar as reasonably necessary for the purposes of obtaining or maintaining insurance coverage, managing risks, obtaining professional advice, or the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.
4.3 We may disclose personal data to our suppliers or subcontractors insofar as reasonably necessary for to deliver our services to you.
4.4 Financial transactions relating to our website and services are handled by our payment services providers, gocardless.com, directli.co.uk and stripe.com. We will share transaction data with our payment services providers only to the extent necessary for the purposes of processing your payments, refunding such payments and dealing with complaints and queries relating to such payments and refunds.
4.5 We may disclose your enquiry data to one or more of those selected third party suppliers of goods and services identified on our website for the purpose of enabling them to contact you so that they can offer, market and sell to you relevant goods and/or services. Each such third party will act as a data controller in relation to the enquiry data that we supply to it; and upon contacting you, each such third party will supply to you a copy of its own privacy policy, which will govern that third party's use of your personal data.
4.6 In addition to the specific disclosures of personal data set out in this Section 4, we may disclose your personal data where such disclosure is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person. We may also disclose your personal data where such disclosure is necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

5. International transfers of your personal data
5.1 In this Section 5, we provide information about the circumstances in which your personal data may be transferred to countries outside the European Economic Area (EEA).

5.2 We and our other group companies have facilities and sub-contractors in the United States of America. The European Commission has made an "adequacy decision" with respect to the data protection laws of each of these countries. Transfers to each of these countries will be protected by appropriate safeguards, namely the use of standard data protection clauses adopted or approved by the European Commission.

5.3 We may from time to time have subcontractors that are situated outside of the EAA and in countries where the European Commission has deemed the countries as "non-adequate countries". Article 13(1)(f) of the GDPR requires that data controllers disclose to data subjects "where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 transfers subject to appropriate safeguards or 47 binding corporate rules, or the second subparagraph of Article 49(1) limited transfers for compelling legitimate interests, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available".

6. Retaining and deleting personal data

6.1 This Section 6 sets out our data retention policies and procedure, which are designed to help ensure that we comply with our legal obligations in relation to the retention and deletion of personal data.

6.2 Personal data that we process for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6.3 We will retain your personal data as follows:

(a) For the duration of the service you are subscribed to plus 12 months after you have terminated the service.

6.4 In some cases it is not possible for us to specify in advance the periods for which your personal data will be retained. In such cases, we will determine the period of retention based on the following criteria:

(a) the period of retention of personal data will be determined based on the service that you subscribe to.

6.5 Notwithstanding the other provisions of this Section 6, we may retain your personal data where such retention is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.

7. Amendments

7.1 We may update this policy from time to time by publishing a new version on our website.

7.2 You should check this page occasionally to ensure you are happy with any changes to this policy.

7.3 We may notify you of changes to this policy by email or through the private messaging system on our website.

8. Your rights

8.1 In this Section 8, we have summarised the rights that you have under data protection law. Some of the rights are complex, and not all of the details have been included in our summaries. Accordingly, you should read the relevant laws and guidance from the regulatory authorities for a full explanation of these rights.

8.2 Your principal rights under data protection law are:

(a) the right to access;

(b) the right to rectification;

(c) the right to erasure;

(d) the right to restrict processing;

(e) the right to object to processing;

(f) the right to data portability;

(g) the right to complain to a supervisory authority; and

(h) the right to withdraw consent.

8.3 You have the right to confirmation as to whether or not we process your personal data and, where we do, access to the personal data, together with certain additional information. That additional information includes details of the purposes of the processing, the categories of personal data concerned and the recipients of the personal data. Providing the rights and freedoms of others are not affected, we will supply to you a copy of your personal data.
8.4 You have the right to have any inaccurate personal data about you rectified and, taking into account the purposes of the processing, to have any incomplete personal data about you completed.
8.5 In some circumstances you have the right to the erasure of your personal data without undue delay. Those circumstances include: the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; you withdraw consent to consent-based processing; you object to the processing under certain rules of applicable data protection law; the processing is for direct marketing purposes; and the personal data have been unlawfully processed. However, there are exclusions of the right to erasure. The general exclusions include where processing is necessary: for exercising the right of freedom of expression and information; for compliance with a legal obligation; or for the establishment, exercise or defence of legal claims.
8.6 In some circumstances you have the right to restrict the processing of your personal data. Those circumstances are: you contest the accuracy of the personal data; processing is unlawful but you oppose erasure; we no longer need the personal data for the purposes of our processing, but you require personal data for the establishment, exercise or defence of legal claims; and you have objected to processing, pending the verification of that objection. Where processing has been restricted on this basis, we may continue to store your personal data. However, we will only otherwise process it: with your consent; for the establishment, exercise or defence of legal claims; for the protection of the rights of another natural or legal person; or for reasons of important public interest.
8.7 You have the right to object to our processing of your personal data on grounds relating to your particular situation, but only to the extent that the legal basis for the processing is that the processing is necessary for: the performance of a task carried out in the public interest or in the exercise of any official authority vested in us; or the purposes of the legitimate interests pursued by us or by a third party. If you make such an objection, we will cease to process the personal information unless we can demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the processing is for the establishment, exercise or defence of legal claims.
8.8 You have the right to object to our processing of your personal data for direct marketing purposes (including profiling for direct marketing purposes). If you make such an objection, we will cease to process your personal data for this purpose.
8.9 You have the right to object to our processing of your personal data for scientific or historical research purposes or statistical purposes on grounds relating to your particular situation, unless the processing is necessary for the performance of a task carried out for reasons of public interest.
8.10 To the extent that the legal basis for our processing of your personal data is:
(a) consent; or
(b) that the processing is necessary for the performance of a contract to which you are party or in order to take steps at your request prior to entering into a contract,
and such processing is carried out by automated means, you have the right to receive your personal data from us in a structured, commonly used and machine-readable format. However, this right does not apply where it would adversely affect the rights and freedoms of others.

8.11 If you consider that our processing of your personal information infringes data protection laws, you have a legal right to lodge a complaint with a supervisory authority responsible for data protection. You may do so in the EU member state of your habitual residence, your place of work or the place of the alleged infringement.
8.12 To the extent that the legal basis for our processing of your personal information is consent, you have the right to withdraw that consent at any time. Withdrawal will not affect the lawfulness of processing before the withdrawal.
8.13 You may exercise any of your rights in relation to your personal data by written notice to us, in addition to the other methods specified in this Section 8.

9. About cookies
9.1 A cookie is a file containing an identifier (a string of letters and numbers) that is sent by a web server to a web browser and is stored by the browser. The identifier is then sent back to the server each time the browser requests a page from the server.
9.2 Cookies may be either "persistent" cookies or "session" cookies: a persistent cookie will be stored by a web browser and will remain valid until its set expiry date, unless deleted by the user before the expiry date; a session cookie, on the other hand, will expire at the end of the user session, when the web browser is closed.
9.3 Cookies do not typically contain any information that personally identifies a user, but personal information that we store about you may be linked to the information stored in and obtained from cookies.

10. Cookies that we use
10.1 We use cookies for the following purposes:
(a) authentication - we use cookies to identify you when you visit our website and as you navigate our website;
(b) status - we use cookies [to help us to determine if you are logged into our website;
(c) personalisation - we use cookies to store information about your preferences and to personalise the website for you;
(d) security - we use cookies as an element of the security measures used to protect user accounts, including preventing fraudulent use of login credentials, and to protect our website and services generally;
(e) advertising - we use cookies to help us to display advertisements that will be relevant to you;
(f) analysis - we use cookies to help us to analyse the use and performance of our website and services and
(g) cookie consent - we use cookies to store your preferences in relation to the use of cookies more generally.

11. Cookies used by our service providers
11.1 Our service providers use cookies and those cookies may be stored on your computer when you visit our website.
11.2 We use Google Analytics to analyse the use of our website. Google Analytics gathers information about website use by means of cookies. The information gathered relating to our website is used to create reports about the use of our website. Google's privacy policy is available at: https://www.google.com/policies/privacy/.

12. Managing cookies

12.1 Most browsers allow you to refuse to accept cookies and to delete cookies. The methods for doing so vary from browser to browser, and from version to version. You can however obtain up-to-date information about blocking and deleting cookies via these links:

(a) https://support.google.com/chrome/answer/95647?hl=en (Chrome);

(b) https://support.mozilla.org/en-US/kb/enable-and-disable-cookies-website-preferences (Firefox);

(c) http://www.opera.com/help/tutorials/security/cookies/ (Opera);

(d) https://support.microsoft.com/en-gb/help/17442/windows-internet-explorer-delete-manage-cookies (Internet Explorer);

(e) https://support.apple.com/kb/PH21411 (Safari); and

(f) https://privacy.microsoft.com/en-us/windows-10-microsoft-edge-and-privacy (Edge).

12.2 Blocking all cookies will have a negative impact upon the usability of many websites.

12.3 If you block cookies, you will not be able to use all the features on our website.

13. Our details

13.1 This website is owned and operated by Catapult Training Limited.

13.2 We are registered in England and Wales under registration number, 5086974, and our registered office is at 48 Alderney House, Ferry Court, Cardiff, CF11 0JT.

13.3 Our principal place of business is at 48 Alderney House, Ferry Court, Cardiff, CF11 0JT.

13.4 You can contact us:

(a) by post, to the postal address given above;

(b) using our website contact form;

(c) by email, using the email address published on our website from time to time.

14. Data protection officer

14.1 Our data protection officer's is the Managing Director and can be contacted at support@catapultsolutions.co.uk

Roles And Responsibilities

Within the data protection framework relevant to our compliance with the GDPR, the following major roles need to be defined and allocated:

- Data Controller
- Data Processor
- Information Security Manager
- Data Protection Officer

Catapult Training Limited are "data controllers" when we process information about our partners account e.g. crm and accounts.

Catapult Training Limited are "data processors" of any data that our partners provide to us e.g. information regarding their business. We see ourselves primarily as "data processors".

The Information Security Manager and The Data Protection Officer is the Managing Director.

Data Controller

Although in general Catapult Training Limited is considered a Data Processor rather than a Data Controller this will apply on occasion.

The GDPR defines a "controller" as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data". Accordingly, the responsibilities described below may be assigned to an individual or may be taken to apply to the organisation as a whole.

The Data Controller has the following responsibilities:

- Ensure that the principles relating to processing of personal data described in Article 5 of the GDPR are adhered to and be able to demonstrate compliance with them. In summary, these are to ensure that personal data are:

  processed lawfully, fairly and transparently
  collected for specified, explicit and legitimate purposes
  adequate, relevant and limited to what is necessary
  accurate and, where necessary, kept up to date
  kept in a form which permits identification of data subjects for no longer than is necessary
  processed in a manner that ensures appropriate security

- Ensure that the consent of the data subject to processing of personal data is obtained where appropriate, including parental consent for children

- Provide all of the information required under the GDPR to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language

- Facilitate the exercise of data subject rights under the GDPR and keep the data subject informed of the progress of their request

- Implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR

- Ensure that only processors who provide sufficient guarantees to implement appropriate technical and organisational measures to meet the GDPR and protect personal data, are used

- Maintain a record of processing activities related to personal data which fall under the controller's responsibility

- Cooperate, on request, with the supervisory authority in the performance of its tasks

- Ensure that any person acting under the authority of the controller who has access to personal data does not process them except on instructions from the controller

- Notify a personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, in accordance with organisational procedures

- Document any personal data breaches, including the facts relating to the personal data breach, its effects and the remedial action taken

- Where appropriate, communicate a personal data breach to the data subject without undue delay

- Carry out data protection impact assessments, where appropriate, in accordance with procedures

- Designate a data protection officer where required by the GDPR, publish their details and communicate them to the supervisory authority

- Support the data protection officer in performing their tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge

- Transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available

Data Processors

Catapult Training Limited sees itself principally as a Data Processor.

The GDPR defines a "processor" as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller". Therefore, the responsibilities described below may be assigned to an individual or may be taken to apply to the organisation as a whole.

The Data Processor has the following responsibilities:

- Ensure that all processing of personal data is governed by a contract or other legal act that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller

- Process the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation

- Ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality

- Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk associated with the processing of personal data

- Obtain the prior specific or general written authorisation of the controller before engaging another processor

- Assist the controller in the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights

- Delete or return all the personal data to the controller after the end of the provision of services relating to processing

- Make available to the controller all information necessary to demonstrate compliance with the obligations laid down in the GDPR and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller

- Maintain a record of all categories of processing activities carried out on behalf of a controller

- Cooperate, on request, with the supervisory authority in the performance of its tasks

- Ensure that any person acting under the authority of the processor who has access to personal data does not process them except on instructions from the controller

- Notify the controller without undue delay after becoming aware of a personal data breach

- Designate a data protection officer where required by the GDPR, publish their details and communicate them to the supervisory authority

- Support the data protection officer in performing their tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge

Data Protection Officer

The Data Protection Officer is a required appointment in line with the EU General Data Protection Regulation and has specific responsibilities for the protection of the personal data of data subjects.

A Data Protection Officer is required in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale;

or

(c) the core activities of the controller or the processor consist of 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.

The Data Protection Officer has the following responsibilities:

- Inform and advise the data controller or the processor and the employees who carry out processing of their obligations under applicable data protection law

- Monitor compliance with data protection law and with the policies of the data controller or processor in relation to the protection of personal data

- Assignment of responsibilities, awareness-raising and training of staff involved in the processing of personal data, and the related audits

- Provide advice where requested regarding data protection impact assessments and monitor their performance

- Cooperate with all relevant supervisory authorities for data protection

- Act as the contact point for supervisory authorities on issues relating to personal data processing and to consult, where appropriate, with regard to any other matter

Information Security Manager

The Information Security Manager is the primary role with a dedicated focus on information security and related issues.

The Information Security Manager has the following responsibilities:

- Reporting to management on all security related matters on a regular and ad-hoc basis when required
- Communicate the information security policy to all relevant interested parties where appropriate, including customers
- Implement the requirements of the information security policy
- Manage risks associated with access to the service or systems
- Ensure that security controls are in place and documented
- Quantify and monitor the types, volumes and impacts of security incidents and malfunctions
- Define improvement plans and targets for the financial year
- Monitor achievement against targets
- Identify and manage information security incidents according to a process

Information Security Manager

A register is kept for the following:

1. Data Subject Request Register - this will maintain a list of any requests made for the data we hold on an individual.

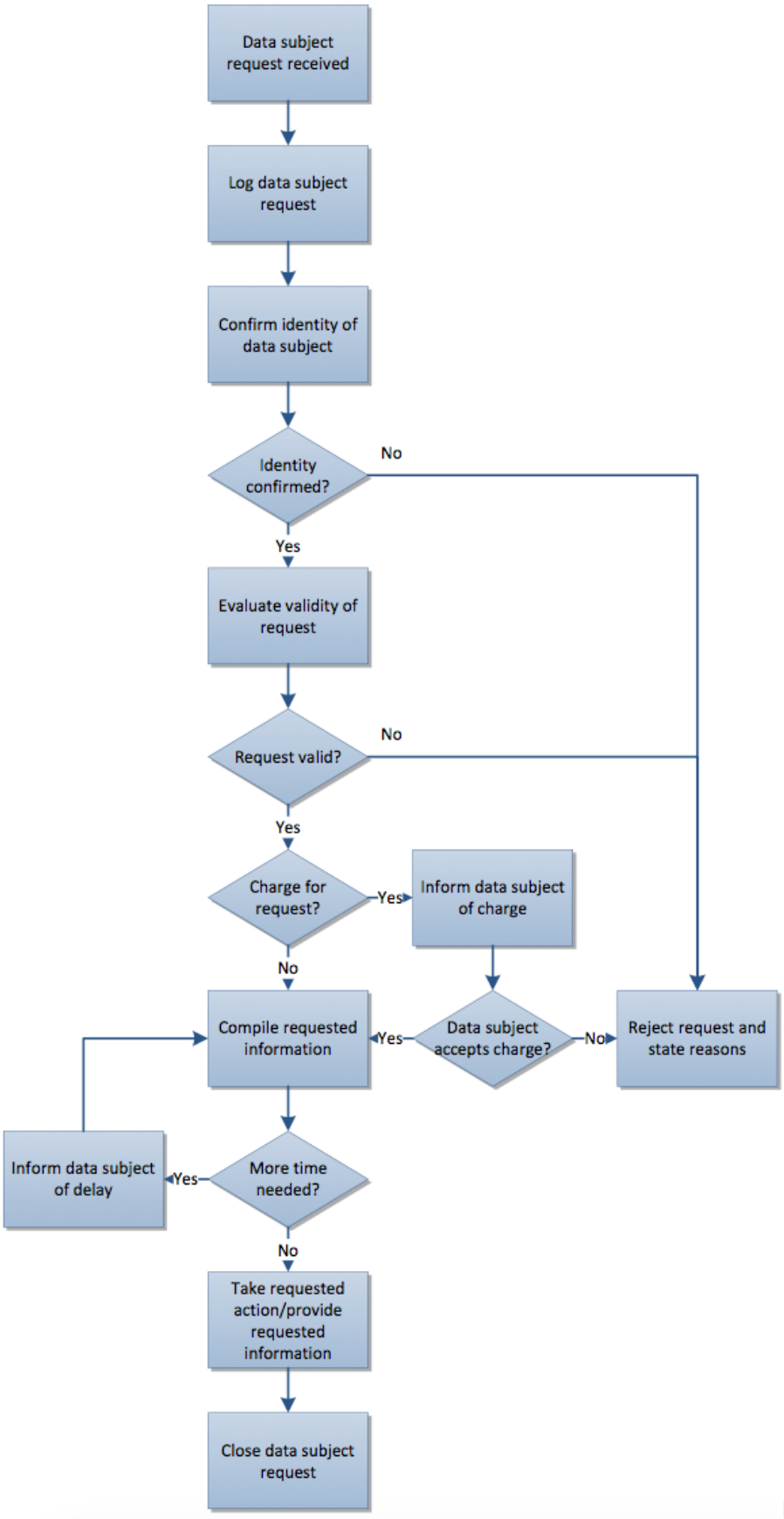
2. Personal Data Breach Register - this will maintain a list of any breaches of personal data.

Data Protection Impact Assessment

A data protection impact assessment has been carried out and is reviewed regularly.

Data Subject Request Procedure

In order to carry out a data subject request then the applicant needs to send a request to support@catapultsolutions.co.uk - the following process will be carried out.



Data Breach Procedure

It is a requirement of the EU General Data Protection Regulation 2016 (GDPR) that incidents affecting personal data that are likely to result in a risk to the rights and freedoms of data subjects must be reported to the data protection supervisory authority without undue delay and where feasible, within 72 hours of becoming aware of it. In the event that the 72-hour target is not met, reasons for the delay must be given.

Where an incident affects personal data, a decision must be taken regarding the extent, timing and content of communication with data subjects. The GDPR requires that communication must happen "without undue delay" if the breach is likely to result in "a high risk to the rights and freedoms of natural persons".

ONCE A BREACH HAS OCCURRED

Once it has been decided that a breach of personal data has occurred, there are two parties who may be required by the GDPR to be informed. These are:

1. The supervisory authority
2. The data subjects affected

It is not a foregone conclusion that the breach must be notified; this depends upon an assessment of the risk that the breach represents to "the rights and freedoms of natural persons" (GDPR Article 33). The following sections describe how this decision must be taken and what to do if notification is required.

The supervisory authority is the Information Commissioners Office.

DECIDING ON NOTIFYING THE SUPERVISORY AUTHORITY

The GDPR states that a personal data breach shall be notified to the supervisory authority "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons" (GDPR Article 33). This requires that the organisation assess the level of risk before deciding whether or not to notify.

Factors to be taken into account as part of this risk assessment should include:

- Whether the personal data was encrypted
- If encrypted, the strength of the encryption used
- To what extent the data was pseudonymised (i.e. whether living individuals can reasonably be identified from the data)
- The data items included e.g. name, address, bank details, biometrics
- The volume of data involved
- The number of data subjects affected
- The nature of the breach e.g. theft, accidental destruction
- Any other factors that are deemed to be relevant

Parties involved in this risk assessment may include representatives from the following areas, depending on the nature and circumstances of the personal data breach:

- Senior management
- Business area(s)
- Technology
- Information security
- Legal
- Data protection officer
- Others

The risk assessment method, its reasoning and its conclusions should be fully documented and signed off by top management. The result of the risk assessment should include one of the following conclusions:

1. The personal data breach does not require notification
2. The personal data breach requires notification to the supervisory authority only
3. The personal data breach requires notification both to the supervisory authority and to the affected data subjects

These conclusions may be subject to change based on feedback from the supervisory authority and further information that is discovered as part of the ongoing investigation of the breach.

DECIDING ON NOTIFYING THE DATA SUBJECT

The GDPR states that a personal data breach shall be notified to the data subject"when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons" (GDPR Article 34).Note the addition of the word "high" over and above the definition given in Article 33.

The risk assessment carried out earlier in this procedure (section 2.1.1) will have determined whether the risk to the rights and freedoms of the data subjects affected is judged to be sufficiently high to justify notification to them.

However, if measures have subsequently been taken to mitigate the high risk to the data subjects, so that it is no longer likely to happen, then communication to the data subjects is not required by the GDPR.

Notification to affected data subjects is also not mandated by the GDPR where it "would involve disproportionate effort" (GDPR Article 34). However, in this case a form of public communication should be used instead.
Again, this may change based on feedback from the supervisory authority and further information that is discovered as part of the ongoing investigation of the breach.

In most cases it will be appropriate to notify affected data subjects via letter or email or both in order to ensure that the message has been received and that they have an opportunity to take any action required.

Once it has been decided that the breach justifies communication to the data subjects affected, the GDPR requires that this be done without undue delay.

The communication to the affected data subjects "shall describe in clear and plain language the nature of the personal data breach" (GDPR Article 34) and must also cover:

a) Name and contact details of the data protection officer or other contact point where more information may be obtained

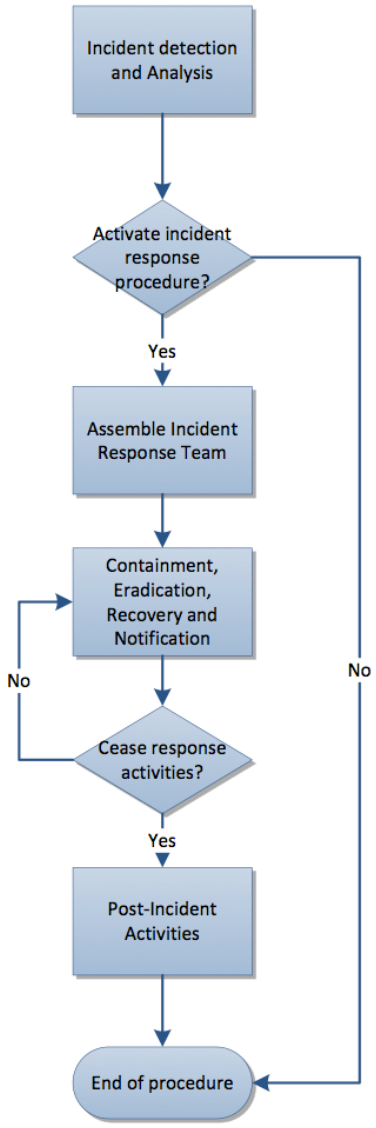
b) A description of the likely consequences of the personal data breach

c) A description of the measures taken or proposed to be taken to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects

In addition to the points required by the GDPR, it may be appropriate to offer advice to the data subject regarding actions they may be able to take to reduce the risks associated with the personal data breach.

Security Incident Response

In the event of a security incident the Managing Director should be informed as soon as possible by emailing support@catapultsolutions.co.uk. The following procedure will be followed.



DETECTING AN INCIDENT

An incident may be initially detected in a wide variety of ways and through a number of different sources, depending on the nature and location of the incident. Some incidents may be self-detected via software tools used within the company or by employees noticing unusual activity. Others may be notified by a third party such as a customer, supplier or law enforcement agency who has become aware of a breach perhaps because the stolen information has been used in some way for malicious purposes.

It is not unusual for there to be a delay between the origin of the incident and its actual detection; one of the objectives of a proactive approach to information security is to reduce this time period. The most important factor is that the incident response procedure must be started as quickly as possible after detection so that an effective response can be given.

Once the incident has been detected, an initial impact assessment must be carried out in order to decide the appropriate response.

This impact assessment should estimate:

- The extent of the impact on IT infrastructure including computers, networks, equipment and accommodation
- The information assets (including personal data) that may be at risk or have been compromised
- The likely duration of the incident i.e. when it may have begun
- The business units affected and the extent of the impact to them
- For breaches affecting personal data, the degree of risk to the rights and freedoms of the data subjects
- Initial indication of the likely cause of the incident

This information should be documented so that a clear time-based understanding of the situation as it emerges is available for current use and later review.

A list of the information assets (including personal data), business activities, products, services, teams and supporting processes that may have been affected by the incident should be created together with an assessment of the extent of the impact.

As a result of this initial analysis, any member of the management team has the authority to contact the Managing Director at any time to ask him/her to assess whether the Incident Response Procedure should be activated.

Contacting Our Team

You can contact our team to address any incorrect information, withdraw consent or any other enquiry such as a data subject request with regards to the information we hold by contacting:

support@catapultsolutions.co.uk


Catapult.