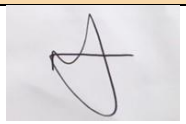
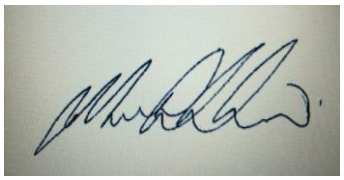
DATA PROTECTION (GDPR) POLICY
2018-2019

Prepared By:	Authorised by
PAUL DREW / MARK SIMPKINS	PAUL DREW
Date Sanctioned	NOVEMBER 2018
SIGNATURE/S:	

Board Signatures


PAUL DREW


MARK FITCHEW

Background

All Apprentify employees, temporary staff, consultants, contractors and third parties have a duty to protect Apprentify data that they create, store, process or transfer.

The UK Data Protection Act 1998 [6] and French Data Protection Act [7] will be superseded by the EU General Data Protection Regulation [8] (GDPR) on 25th May 2018. At a minimum, Apprentify must ensure data protection standards within the company meet these regulations. The following document sets out the requirements for Apprentify employees, third parties and other stakeholders, to fulfil these regulatory obligations.

Purpose

The purpose of this document is to specify and communicate to all personnel the APPRENTIFY policy on data protection. In particular:

- To ensure data protection good practice across the organisation;
- To ensure compliance with GDPR [8] and other applicable legislation and regulation related to personal data.

This document outlines internal policy in respect of data handling, but this policy is subject to all the laws, rules and regulations that Apprentify is governed by. In the event this policy allows employees of Apprentify to exercise discretion, such discretion must be exercised within the confines of Apprentify statutory obligations and must not contravene any of its legal, accounting or other regulatory requirements.

Scope

This policy applies to all Apprentify personnel irrespective of status, including temporary staff, contractors, consultants, and third parties.

Statement of Policy

It is the policy of Apprentify to ensure that all data shall be protected in proportion to the sensitivity of the data, and in line with all legal and regulatory requirements.

Requirements

General

All data created, stored, processed and transferred by personnel shall have a classification in accordance with the Apprentify Data Classification Policy [2].

Following its classification, all data shall be handled with respect to the Apprentify Data Handling Policy [3].

Personal Data

Personal data shall be protected by the implementation of appropriate technical and organisational measures and integration of necessary safeguards, considering:

- the state of the art;
- the cost of implementation;
- the nature, scope, context and purposes of processing the data; and
- the risks to rights and freedoms of persons posed by the processing.

Appropriate technical and organisational measures shall be implemented for ensuring that, by default, personal data:

- personal data collection is limited to that which are necessary for each specific purpose of the processing;
- personal data processing is limited to that which are necessary for each specific purpose of the processing;
- personal data access is limited to that which are necessary for each specific purpose of the processing;
- the storage period of all personal data is limited to that which are necessary for each specific purpose of the processing.

All personnel shall ensure that the Data Protection Officer (DPO) is involved/data protection advice is sought where needed in all issues which relate to the protection of personal data in a properly and in a timely manner.

Data Protection Officer

Apprentify shall always have a designated Data Protection Officer (DPO)

All personnel shall support the DPO in performing his/her tasks, these tasks shall be carried out without influence on or consequence to the DPO and without any conflict of interest.

The DPO shall be designated based on (amongst other capabilities) professional qualities and expert knowledge of data protection law and practices.

Apprentify shall publish the contact details of the DPO and communicate them to the relevant data protection supervisory authority (The Information Commissioner's Office in the UK and Commission Nationale de l'Informatique et des Libertés – CNIL in France).

The DPO shall have at least the following tasks:

- to inform and advise Apprentify and its employees who carry out processing of their obligations pursuant to GDPR [8] and other data protection provisions;
- to monitor compliance with GDPR [8], other data protection provisions and Apprentify policies in relation to the protection of personal data;
- to provide advice where requested as regards the data protection impact assessment and monitor its performance;
- to cooperate with the supervisory authorities;
- to act as the contact point for the supervisory authorities on issues relating to personal data processing.

Roles and Responsibilities

All personnel are responsible for the records they create, use and store.

Managers are directly responsible for implementing this policy within their functional areas, and for adherence by their staff.

The Data Protection Officer has direct responsibility for maintaining this policy and providing advice on implementation.

Definitions

1. ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

2. ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

3. ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future;

4. ‘profiling’ means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

5. ‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

6. ‘controller’ means 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

7. ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

8. ‘recipient’ means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

9. ‘consent’ of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Data Protection Impact Assessment

Background

The UK Data Protection Act 1998 [3] will be superseded by the EU General Data Protection Regulation [4] (GDPR) on 25 May 2018. At a minimum, Apprentify must ensure data protection standards within the company meet these regulations. The following document sets out the requirements for Apprentify employees, third parties and other stakeholders, to fulfil these regulatory obligations.

One aspect of the GDPR is the requirement for 'Data Protection by Design and by Default', this means that Privacy must be considered from the commencement of any initiative and throughout the lifecycle of our processes. A mandatory requirement is the creation of Data Protection Impact Assessments within the business which are needed when there is an initiative (e.g. a project or process) which places a high risk regarding privacy on the data of individuals.

This form has been created alongside guidance within the GDPR to create a Data Protection Impact Assessment.

Purpose

The purpose of this document is to create a template that will be populated by Apprentify in the event of a Data Protection Impact Assessment being required.

Where this policy allows employees of Apprentify to exercise discretion, such discretion must be exercised within the confines of Apprentify statutory obligations and must not contravene any of its legal, accounting or other regulatory requirements.

Scope

The form applies to all Apprentify initiatives (projects, processes, applications, systems and contracts).

Statement of Policy

Our policy is to ensure that all where any new or changed initiatives are identified within the business that they are assessed to identify whether a Data Protection Impact Assessment is required. If the Data Protection Impact Assessment is required, this template should be used.

If the Data Protection Impact Assessment is not required (using the validation questions in section 5), this is to be documented and the record of this held by the Data Protection Officer.

Executive Summary

A Data Protection Impact Assessment (DPIA) has been performed on [[INSERT NAME OF PROCESS/APPLICATION/SYSTEM/PROJECT/CONTRACT]]

[[Currently the solution as deployed within Apprentify is limited to storing data such as name, address, contact details, marketing preferences and contact preferences.]]

[[The DPIA was conducted performing interviews with key stakeholders and reviewing documentation provided. Once a complete understanding of the system was consolidated, a review of the information was performed with the stakeholders prior to the key risks and potential solutions being defined. These were then discussed with stakeholders to identify agreed solutions that are documented within the report.]]

[[The agreed solutions have been incorporated into the change programme to be addressed to align with GDPR requirements.]]

Scope

[[The scope of the DPIA included the [PROCESS/APPLICATION/SYSTEM/PROJECT/CONTRACT], both current functionality and that on the roadmap expected to be delivered prior to the implementation of GDPR. Where modules are to be delivered in the future, these were considered in terms of the functionality (and therefore data processed) that is planned to be delivered. Where either internal or external systems or providers interface with [PROCESS/APPLICATION/SYSTEM/PROJECT/CONTRACT], the interface was considered but the other system or provider was not considered within scope.]]

[[The scope excluded tools, solutions and third parties that are separate from the PROCESS/APPLICATION/SYSTEM/PROJECT/CONTRACT platform. This includes solutions or platforms which transmit, receive or process information that is stored, acquired, processed or transmitted by PROCESS/APPLICATION/SYSTEM/PROJECT/CONTRACT.]]

Key Findings and Recommendations

Ref	Type	Finding(s)	Recommendation(s)
1			
2			
3			

Approach

The performance of the DPIA was conducted using the method illustrated in Figure 1:

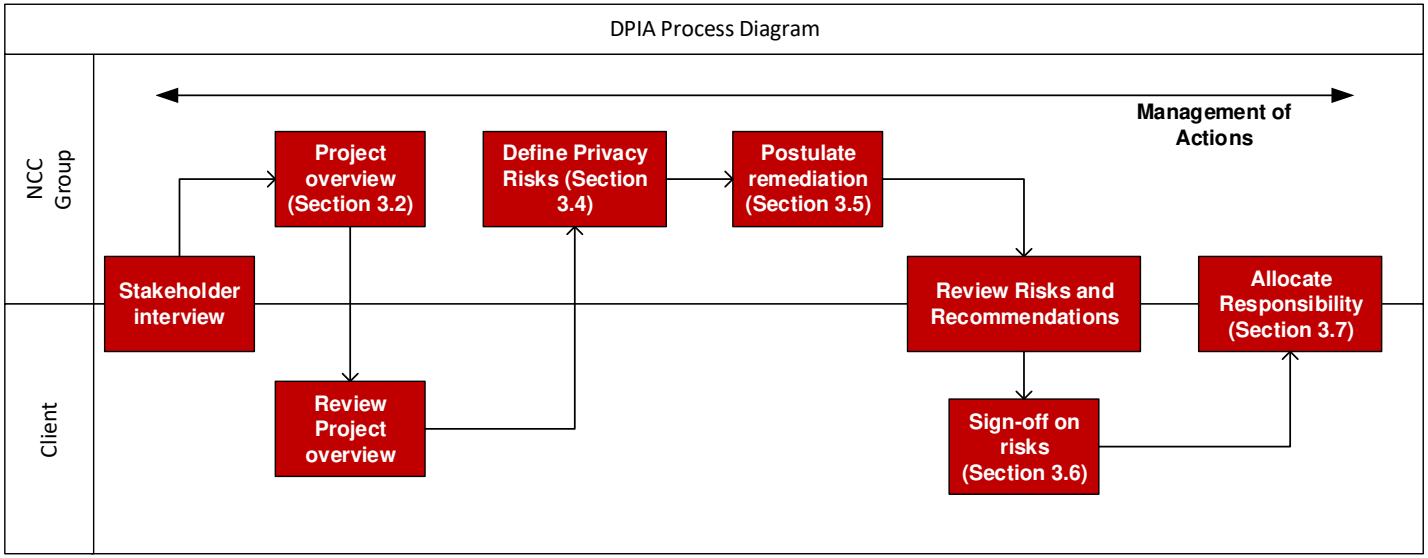


Figure 1: DPIA Process Diagram

As part of the assessment process, the following individuals were interviewed:

Name	Role (e.g., Internal/ External, Job Role)

Need for a DPIA

Under Article 35 (1) of the GDPR which will be enforceable from 25 May 2018, Data Controllers will be required to put mechanisms in place to focus on high risk operations (e.g., extensive automated processing or profiling activities, and processing high amounts of sensitive personal data) regarding personal data and undertake a Data Privacy Impact Assessment to assess the risk introduced by the changes and implement solutions to address these risks.

The GDPR text specifically notes that an assessment is required when:
(a) A systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
(b) Processing on a large scale of special categories of data, or of personal data relating to criminal convictions and offences; or
(c) A systematic monitoring of a publicly accessible area on a large scale.

This DPIA report has been created in line with the ICO PIA Code of Practice, published February 2014, and GDPR Section 3 'Data protection impact assessment and prior consultation'.
The objective of the report is to determine the information flow across the identified project/ process/ system or application and to identify the privacy risks resulting from this. When the risks have been identified, the potential solutions are considered (there may be more than one potential solution to address each risk) before agreeing an approved solution with the organisation.

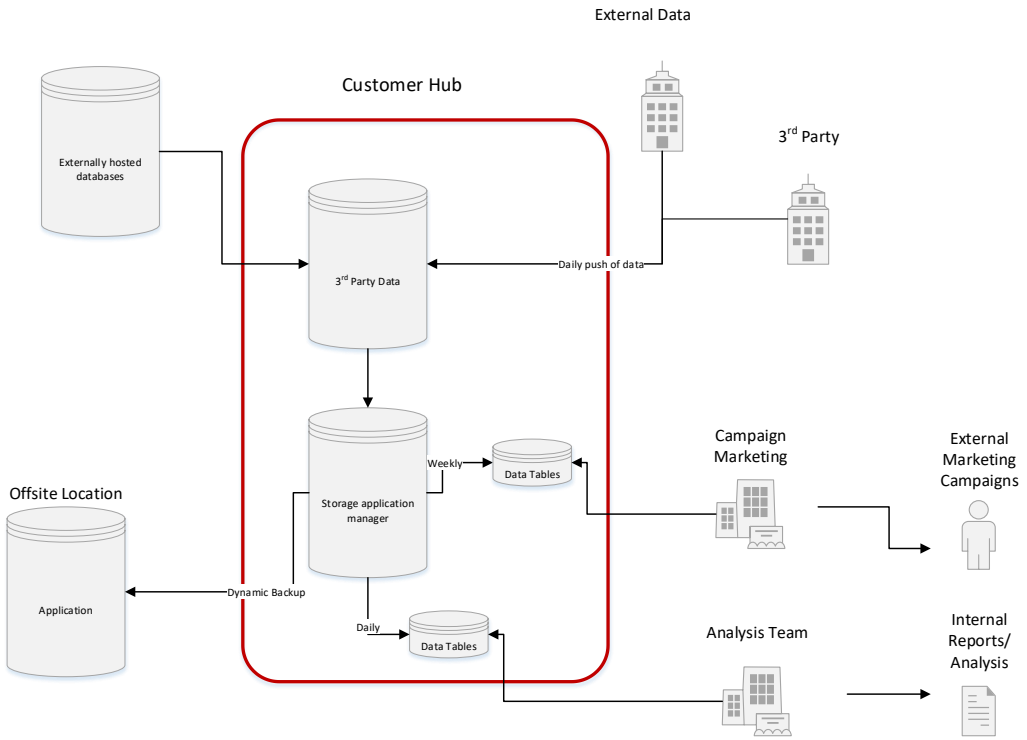
The below screening questions have been considered prior to conducting the DPIA assessment:

Screening Question	Answer Y/N
Does/will the process/application/system/project/contract involve the collection of new information about individuals, either directly or from other sources?	
Does/will the process/application/system/project/contract compel individuals to provide information about themselves, either directly or from other sources?	
Does/will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	
Does/ will the information being collected be shared or stored outside of the European Union?	
Are you/will you be using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?	
Does/will the process/application/system/project/contract involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.	
Does/will the process/application/system/project/contract result in you making decisions or taking action against individuals in ways that can have a significant impact on them?	
Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, information relating to children or special categories of sensitive personal data.	
Does/will the process/application/system/project/contract require you to contact individuals in ways that they may find intrusive?	
Does/will the process/application/system/project/contract require large scale monitoring of public areas?	
Does/will the process/application/system/project/contract entail extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling?	

Project overview

Data flow diagram

This Data Flow Diagram (henceforth referred to as DFD) provides an overview of how the data of individuals is acquired, where it is stored, updated and what it is used for. The individuals depicted represent the start of the data acquisition and the numbers serve as reference for the section below. For a specific description of the individual components found within the application, the data it holds and how it is controlled see Section 3.2.2.



Privacy related project criteria

Ref	Criteria	Detail	Comment(s)
A	Overview (Core Components)		
B	Data Types		
C	Data Acquisition		
D	Data Transfer		
E	Data Processing and Use (Including Consent)		
F	Data Retention		
G	Access Control		
H	Third Parties		
I	Data Security		

Additional Findings

As a result of the interviews, additional risks were identified that fell beyond the scope of the current DPIA. This section briefly outlines the findings as well as the proposed solutions that were made by the stakeholder or during the performance of the DPIA.

Risk	Project/ Process discussed and Concern(s) Highlighted by Stakeholder	Stakeholder Feedback/ Proposed Solution

Privacy and related risks

Note: If the following risks are not addressed, they could result in a failure to meet the requirements of GDPR and, in some circumstances, result in action by the Supervisory Authority.

Under Article 5 of the GDPR, there are six principles relating to the processing of personal data which must be adhered to:

- **Lawfulness, fairness and transparency** – personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject
- **Purpose limitation** – personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- **Data minimisation**- personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed
- **Accuracy** – personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay
- **Retention** – personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject
- **Integrity and confidentiality** – personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

The table below shows the privacy issues and risks identified during this DPIA, along with the relevant principle.

Identifier	Privacy Issue	Relevant Principle	Compliance and Associated Organisation/ Corporate Risk	Potential Impact (Financial, Reputational etc.)
R.1	*There is no formal policy or approach to retention of data across the organization; therefore, data, including personal data is not retained for a specified amount of time.*	*3 – Data Minimisation* *5 - Retention*	*Where there is no defined retention policy within the organisation, individual departments and functions will have different approaches to retaining data. With GDPR there is a need to be clear on the expectation of how long data is retained for and adhere to that policy consistently throughout the organisation (fifth principle of the GDPR). This potentially means that data is being kept for longer than it is needed.* *Additionally this can significantly increase the overall amount of data in the organisation (third principle of the GDPR) and mean increased costs (from storage and backup), increased likelihood that the data is out of date and inaccurate and increased risk in instances where a Right to Access request or Right to Erasure request is made as the organisation will take longer and have higher costs in retrieving all of this data.*	*The impacts on the organisation include;* • *Potential fine under the GDPR for failing to adhere to the Data Minimisation and Retention principle.* • *Potential reputational impact for delays or inability to respond to a Right to Access or Right to Erasure request.*
R.2				
R.3				

Identify Privacy Solutions

Each risk has been allocated a corresponding risk rating. For a breakdown of the risk classification please refer to Annex B.

The potential solutions should be identified including Governance and Technical aspects. The result should show the outcome if the solution is implemented and can be that the risk is accepted, transferred or mitigated.

Identifier	Risk Level	Risk	Solution	Result
R.1	**High**	*With no formal approach to data retention, data could be held within the organisation (both paper and electronic) for either too long or too short a period. This will breach the rights of the data subject under the GDPR in addition to (potentially) excessive data being held which if there is a security breach will result in additional data being compromised.*	*i) A formal data retention policy should be implemented within Value Retail to adhere to firstly regulatory requirements and secondly GDPR requirements. It should be noted that while Value Retail has some discretion regarding retention periods, there will be differing retention periods for data across Value Retail.* *Note: Differing retention periods due to several factors including regulatory requirements (e.g. requirement for retaining financial data is typically seven years, where regulatory requirement for retention of other data may differ) and retention should not keep data for longer than needed (e.g. a CV for an unsuccessful applicant is unlikely to be held for a long period)* *ii) The data retention policy (or other should clearly identify the Value Retail policy towards the removal of data – whether this is either physical removal or anonymising the data in order that it cannot recreated).* *iii) A data inventory should be created to identify all instances of data across the environment (e.g. a person's name may appear in several databases and backups, therefore all instances should be identified in order that they can all be removed or anonymised as needed).*	*If the proposed solutions are implemented the risk will be mitigated.*

			iv) A technical solution will be needed to identify the data as it passes the retention requirements in order that it can be removed. *v) Data Classification should be implemented across Value Retail to assist in determining the approach to securing data at rest and in transit (e.g. which data, if any should be encrypted at rest and in transit).* *vi) A technical solution will be needed should there be a determination to encrypt additional data at rest or in transit.*	
R.2	Medium			
R.3	Low			
R.4	Low			
R.5	**High**			

Sign off and record DPIA Outcomes

Risk Identifier	Solution	Approval Y/N	Reason for Decision	Approved by
R.1				
R.2				
R.3				

Data Protection Committee

The Data Protection Committee (the "Committee") has been established to be the primary forum for overseeing and managing privacy across Apprentify, including driving a privacy aware culture and ensuring that:

- data protection obligations are being met;
- data protection risks are being managed; and
- appropriate policies, processes & frameworks are in place to identify and manage the above effectively.

Membership and Meeting Attendance

- Data Protection Officer (Chair);
- Managing Director
- Marketing Director;
- Head of Sales
- Head of Operations;
- External Data Protection Subject Matter Expert (non-voting)
- Apprentify Board Secretary (Secretary).

A quorum shall be five members which must include the chair (or the chair's nominated deputy) and the secretary. Meetings may be held by telephone and decisions may be made by email once a quorum agrees on a course of action.

Members of staff will be invited to Committee meetings to report on matters arising and give such assistance as the Committee deems necessary. For example, project managers may be invited to provide an overview of a project and to understand the data protection considerations that have been made in implementing it. Note: any such members of staff invited will not have the right to vote.

Frequency of Meetings

The Committee will meet every 2 months and ad hoc meetings will be called as necessary giving notice by email and / or telephone.

All Committee members shall attend all meetings.

The Secretary shall maintain a register of attendance.

Reporting

- Regular reports of key data protection risks and the mitigations in place will be requested by the Committee;
- Reports may be requested from other Committees and management meetings which deal with data protection matters;
- Minutes of Committee meetings shall be circulated promptly to all members of the Committee and to Internal Audit;
- Reports on data protection matters will be circulated as needed to the Audit Committee or other relevant parties.

Authority

The Committee is authorised to direct the investigation of and progress any activity which falls within these terms of reference. It is authorised to seek any information it requires from any employee of the Apprentify and all employees are directed to co-operate with any request made by the Committee. The Committee is further authorised to make decisions that it considers necessary to protect the Apprentify in keeping with the risk appetite of Apprentify.

Legal, and other independent professional advice, as necessary, will be obtained at the discretion of the Committee. The Committee is authorised to obtain outside legal or other independent professional advice and to secure the attendance of outsiders with relevant experience and expertise if it considers this necessary.

The Committee shall have enough resources in order to carry out its duties. These duties are applicable across the whole Apprentify, including joint ventures and associates.

Duties

The duties of the Committee shall be:

- To ascertain and plan for all data protection obligations faced by Apprentify.
- To facilitate the identification of data protection risks.
- To review and oversee data protection risks.
- To review the data protection position of Apprentify and to take action to ensure overall risk exposure is in keeping with the risk appetite of Apprentify.
- To evaluate and manage key data protection themes to identify and implement opportunities to reduce data protection risk exposure in the short and long term.
- To drive continual improvement of data protection in Apprentify.
- To consider any other matter that requires the Committee's attention.
- Any Committee member is able (with approval from the Chair) to call a meeting.
- The Secretary shall send the agenda and any relevant documentation to Committee members (and other relevant parties) no later than 5 business days prior to the meeting.
- The Secretary shall document the minutes of each meeting and circulate to attendees promptly for approval.
- The Audit & Risk Committee will review and approve the Committee's terms of reference annually.
- The Committee will, at least once a year, review its own performance, membership and terms of reference to ensure it is operating at maximum effectiveness and recommend to the Audit & Risk Committee for approval, any changes it considers necessary.

Escalation Procedure

If a disagreement arises over a decision made by the Committee, the issue will be escalated to the Audit Committee to make a final decision. All such issues that require will be included as an agenda item at the next Audit Committee meeting for further review as necessary.

Data Processor Checklist

Background

This checklist has been defined alongside guidance within the EU General Data Protection Regulation [3] (GDPR) to organisations, on areas that should be considered when an organisation uses a third party to process personal data on their behalf.

A data processor is an organisation that holds or process personal data, but does not exercise responsibility for or control over the personal data.

Purpose

The purpose of this document is to define a list of issues and actions that should be considered by Apprentify when using data processors.

Scope

The form applies to all Apprentify data processors.

Statement of Policy

It is the policy of Apprentify that all data processors will be subject to a robust due diligence process prior to being on-boarded in a structured and controlled way.

Requirements

Data processor checklist

The below are area that should be considered by Apprentify when selecting data processors.

Contracts with new data processors;

Note: While the below are detailed for new data processors, all points are relevant for existing data processors and should be considered to retrospectively amend prior to the GDPR becoming enforceable.

- Conduct a review of data processing activities undertaken by third parties in order to have a full list of the data processors used, the data that they are handling and the purposes for the processing they are doing on behalf of Apprentify. This information should be kept in the Data Asset inventory which is a mandated document in GDPR, that must be available if/when requested by a supervisory authority.
- It should be a requirement that data supplied to third parties must remain confidential within those third parties and not be disclosed to other parties without the prior, written consent of Apprentify. In addition, the data must be destroyed when there is no longer a need for it to be retained.
- Any third party who uses sub-contractors to process Apprentify data should be disclosed and adhere to the same data protection obligations as Apprentify requires of the third parties.
- Consider having the data processor indemnify you for any costs incurred in putting right breaches of Data Protection brought about deliberately or negligently by the data processor (ideally including costs of providing support to impacted individuals, even if this is not legally required).
- Require the data processor not to process the data, or allow it to be processed, outside the European Economic Area and, where it wishes to do so, that written approval is obtained from Apprentify in advance of the processing taking place.

Technical and Operational Considerations

- An assessment must be made of the standard of data security in place in relation to data handled by the processor and whether this is aligned to the classification of the data being processed. There should be a requirement that the contract includes the ability of Apprentify to audit the third party to ensure that the technical and operational controls are in place and working effectively (to align with Apprentify Information Security requirements). The security controls required should be risk-based, relevant to the sensitivity of the data and the processing activity(s).
- A mechanism for secure transmission of data between Apprentify and the data processor should be provided.
- A mechanism for you to authorise the activities of the data processor (e.g. specifying which of your staff can issue instructions to the data processor).
- A process should be in place within the data processor for reporting of data security breaches (both internally and to data controllers such as Apprentify). This should include the escalation process to ensure that Apprentify are informed immediately of any actual or suspected security breach they become aware of, irrespective of the cause.
- A process should be in place within the data processor to forward all requests from data subjects (and complaints) to the Apprentify Data Protection Officer without delay.

Roles and Responsibilities

- All personnel have a responsibility to ensure that data processors adhere to the requirements set out in their contracts and escalate to the Data Protection Officer when they believe that the data processor is not adhering to these requirements.
- Managers are directly responsible for implementing the policy and standards within their functional areas, and for adherence by their staff.
- The Legal Department has direct responsibility for maintaining contracts with Data Processors and for ensuring that these are updated as required to align with GDPR requirements.
- The procurement department has direct responsibility for ensuring that within the procurement process the noted considerations are considered.
- The Internal Audit department are directly responsible for auditing third party data processors using a risk-based approach within the Internal Audit plan.
- The Data Protection Officer has direct responsibility for maintaining this document and providing advice on implementation.

