Kickstart
the moped hire charity

Personal Data processing policy

Kickstart Norfolk

20 June 2018

Table of Contents

Document Control

Version	Date	Author	Comments
1.0	31 May 2018	George Holmes	Prepared by Idvallo Solutions
1.1	20 June 2018	George Holmes	Updated with minor changes following review meeting with Kickstart

Introduction

Implementing and observing robust Data Protection policies supports compliance with British Data Protection legislation.

This policy describes how Personal Data should be collected from:

- Employees.
- Service users and prospective service users.
- Any other parties.

and details what compliance measures are necessary at the point of collection and for further use.

Collecting Personal Data

Personal Data must not be collected or acquired unless all of the following conditions are true:

- The purpose (or purposes) for which the business requires the Personal Data is described in the Personal Data Taxonomy.
- The Personal Data falls within one of the categories outlined in the Personal Data Taxonomy.
- The recipients (or categories of recipients) with which the Personal Data may be shared or disclosed are identified in the Personal Data Taxonomy.
- A legal basis supporting the acquisition of the Personal Data is outlined in the Personal Data Taxonomy.
- Where the Personal Data will be transferred or stored outside the United Kingdom, the country and party receiving the Personal Data is listed in the Personal Data Taxonomy, with corresponding safeguards given separately in this policy.
- The source of the Personal Data is authorised by this policy.
- Any automated decision making or profiling is supported in the approved list found later in this policy.
- When the Personal Data is required in support of a statutory or contractual requirement, the possible consequences of not providing the Personal Data are understood and described in this policy.

A Privacy Notice must also be issued as described in Right to be informed in the Rights guaranteed to individuals section that follows.

Additional Personal Data

From time to time, additional Personal Data (the collection and processing of which is not authorised by this policy) may be collected or processed. An example of this would be a customer voluntarily disclosing Personal Data concerning their health in an account management conversation.

When additional Personal Data not authorised by this policy is collected from an employee, prospective service user, service user or supplier, the following approach should be taken:

When additional Personal Data is otherwise collected

Any other additional Personal Data that may be collected or processed must immediately be erased once the unauthorised collection or processing is discovered.

All physical and electronic copies (including any recordings) must be securely erased.

Retaining Personal Data

The Personal Data Taxonomy specifies the retention period for Personal Data and is aligned with the Privacy Notices in use at Kickstart Norfolk.

An individual may invoke their Right to restrict processing on their Personal Data. This could legally require the retention of their Personal Data beyond the documented retention period. The rationale for this right is that the individual may require the Personal Data in support of a legal claim.

Rights guaranteed to individuals

Right to be informed

Where Personal Data has been directly collected, Privacy Notices must be made available to the individual(s) who provided the information.

In cases where Personal Data has not been directly collected:

- There must be valid and documented legal basis for the acquisition from the individual(s) whose Personal Data has been provided.
- A Privacy Notice must be given to the individuals whose Personal Data has been provided within one month; or if the Personal Data will be used to communicate with the individual(s) who provided it when this first occurs.
- If the Personal Data will be disclosed to another recipient, a Privacy Notice must be issued to the individual(s) who provided the Personal Data before the disclosure occurs.
- Where Personal Data has not been directly collected, the source(s) of the Personal Data must be outlined in issued Privacy Notices, including details on publicly-accessible sources (where relevant).

Right to restrict processing

When processing of Personal Data has been restricted, it can be stored, but no further processing of it can occur.

Processing of Personal Data should be restricted in the following circumstances:

- When an individual has asked for a correction to be made to their Personal Data (Right to rectification) or has otherwise contested accuracy.
- If an objection to processing on grounds of legitimate interests, in the public interest or for the exercise of official authority has been received.
- If processing has been shown to be unlawful and the individual whose Personal Data is affected has requested restriction over erasure.

Should a restriction on the processing of Personal Data be lifted, the individual concerned must be advised that the restriction is no longer in force.

Restriction of processing is also covered as part of the workflows for these processes:

- Right to rectification.
- Right to object.

Rights related to automated decision making

These rights apply when a decision producing a legal effect (or similar) on an individual is made through automated processing of their Personal Data, although they **do not apply** when:

- The automated decision making is necessary for creating or operating a contract with the individual.
- The automated decision making is authorised by law (ie. fraud detection).
- The individual has granted explicit consent for the automated decision making.

When these rights have been invoked by an individual, you must:

- Provide human intervention in the associated decision-making process, including dialogue with the affected individual.
- Allow the affected individual to express their point of view.
- Provide the affected individual with an explanation of how the decision was reached and allow them to challenge it.

Automated decisions must not:

- Concern a child.
- Involve the processing of special categories of data unless the affected individuals have given their explicit consent or there is substantial public interest (on the basis of UK or EU law).

Rights relating to profiling

Processing for profiling must be fair and transparent. The logic involved must be documented in a meaningful way and made available to affected individuals by way of inclusion in a Privacy Notice. The Privacy Notice must also outline the significance and any consequences of the profiling.

Profiling has to use suitable mathematical or statistical procedures.

Technical and business processes must be in place to allow the straightforward correction of inaccuracies and minimise the risk of errors.

Personal Data used in profiling must be secured according to the risk posed to the interest and rights of individuals while preventing any discriminatory effects.

Other rights

Refer to the current processes in force at Kickstart Norfolkfor details on the workflows used to guarantee the following rights to individuals:

- Right of access.
- Right to rectification.
- Right to erasure.
- Right to object.
- Right to data portability.

Marketing calls

Live calls

Live marketing telephone calls must not be placed to people when any of the following conditions apply:

- Their telephone number appears on the Kickstart Norfolk suppression list.
- Their telephone number is registered with the Telephone Preference Service (TPS) or the Corporate Telephone Preference Service (CTPS) – unless they explicitly opted-in to receive marketing calls.

When live marketing calls are made:

- The business's and caller's name must be given.
- The business's telephone number (or alternative contact number) must be displayed to the person receiving the call, where their telephone supports this.
- A contact address or freephone number must be provided if requested by the person receiving the call.

Automated calls

Automated marketing calls must not be placed unless the recipient has provided explicit consent to receive them.

When automated marketing calls are made:

- The business's name must be announced.
- A contact address or freephone number must be announced.
- The business's telephone number (or alternative contact number) must be displayed to the person receiving the call, where their telephone supports this.

Marketing faxes

Faxes must not be sent for marketing purposes.

Marketing lists

Business to Consumer (B2C)

This category will include any marketing lists carrying details of private individuals, sole traders or partnerships.

The broker or agent selling B2C marketing lists to the business must be able to demonstrate that everyone on list have given their consent for their Personal Data to be shared with Kickstart Norfolk; and specific consent has been granted for marketing by telephone, post and email, according to which of these mediums the member of the marketing list has opted in to.

Records should be kept of each list purchased, along with evidence of consent granted by everyone on the list for their Personal Data to be shared with Kickstart Norfolk.

Business to Business (B2B)

B2B marketing lists feature contacts employed by limited companies, public limited companies and other corporate bodies (such as public sector organisations).

The broker or agent selling B2B marketing lists to the business must be able to demonstrate that they have populated the list in and fair and lawful way. This demonstration must include an explanation of the lawful basis (which will most likely be legitimate interest) that supports the use of all Personal Data in the list.

If a B2B marketing list has been populated using consent as the lawful basis, the broker or agent selling the list must provide evidence that everyone on list have given their consent for their Personal Data to be shared with Kickstart Norfolk; and specific consent has been granted for marketing by telephone, post and email, according to which of these mediums the member of the marketing list has opted in to.

Records should be kept of each list purchased, along with evidence of consent granted by everyone on the list for their Personal Data to be shared with Kickstart Norfolk (where consent has been used to populate the list).

Websites & cookies

The Kickstart Norfolk website should carry:

- A Privacy policy
- A Cookies policy
- A “cookie consent” popover/dialog used to obtain a website user’s consent for the use of cookies.

Marketing emails (electronic messages)

Except for LinkedIn, direct messages sent on social media and similar platforms for marketing purposes fall within the scope of legislation governing marketing emails and must be sent in accordance with this policy.

Electronic messages include emails, text messages and direct messages on social media (except LinkedIn).

Marketing electronic messages must not be sent if the recipient's address appears on the suppression list.

One of the following conditions must be true for an electronic marketing message to be sent legally if the recipient does not appear on the suppression list:

- The recipient has opted-in to receive marketing electronic messages.
- The recipient is an existing customer or client who has purchased a similar product or service to that being marketed, in the past.
- The recipient is a prospective customer who has previously negotiated to buy a similar product or service to that being marketed.
- The recipient is an employee of a corporate body (limited company, public limited company, public sector organisation etc).

When relying on the recipient being an existing or prospective customer as above, the individual must have been given a simple way to opt out of marketing electronic messages:

- When their address was first collected.
- In every electronic marketing message they have been sent.

If the recipient was not presented with a simple way to opt out of previous electronic marketing messages, they cannot be legally marketed to by electronic message on the basis they are an existing or prospective customer, unless they have separately opted-in to receive electronic message marketing.

The business's name must be clearly displayed in each marketing electronic message sent along with a valid contact (email) address and a simple way for the recipient to opt-out or unsubscribe.

Marketing to consumers and businesses outside the United Kingdom

The previous sections have covered the various rules and regulations for marketing to UK-based consumers and businesses.

When marketing to consumers and businesses outside the UK (for example in the European Union):

- The company is bound by the prescriptions of the GDPR as interpreted by the ICO, which are covered by this policy document.
- The company is bound by the prescriptions of the PECR as interpreted by the ICO, as covered by this document.
- The company should comply with any specific local Data Protection laws in the country where the prospect or customer is based.

Data Protection laws specific to a prospect's or customer's country may be more restrictive than the ICO's interpretation of the GDPR and PECR in the UK. For example, Germany's local Data Protection laws require opt-in (consent) before marketing emails can be sent to B2B contacts at corporate bodies, where as this is permissible on an opt-out (no upfront consent required) basis in the UK.

Where local laws are more restrictive than the UK, alternative approaches to marketing (or collecting consent for marketing) should be considered, including:

- Using telemarketing (where permissible) to make first contact with a prospect, with a view to securing consent for email marketing and/or converting the prospect to a customer.
- Using LinkedIn to establish initial contact with a prospect and secure their consent for the use of other marketing channels (email, telephone etc).

When collecting prospect details from non-UK B2B contacts at trade fairs (whether in the UK or not) or similar events, it is recommended that consent is obtained for marketing by email and telephone if the contact is based in a country with restrictive Data Protection laws. Consent collected in this way should be documented as part of the normal Data Protection record-keeping carried out by the business.

Sources of Personal Data

Other than direct collection, these are the only authorised sources of Personal Data:

- Marketing lists purchased from brokers who have assured their provenance.
- Publicly-available and free-to-search directories such as LinkedIn, public websites etc.
- Professional advisers (ie. Occupational Health, Company Doctor) retained by the business.
- An employee's General Practitioner or otherwise responsible medical professional.
- Suppliers to the business, where the Personal Data is required to support the delivery of their product or service.
- Sponsors, funding bodies or other organisations who refer service users to Kickstart Norfolk

When Personal Data is collected, a record should be made of:

- The source of the Personal Data (from the list above).
- The date the Personal Data was collected or acquired.
- Where the Personal Data was collected directly from the person described by it, their name.

These records should be:

- Attached to the relevant CRM record for service users.
- Stored in an employee's HR file, where employee Personal Data is collected.
- Kept with supplier records, in the case where supplier contact Personal Data has been acquired.

Keeping Personal Data up to date

As a general rule, all Personal Data should be pro-actively checked for correctness by the business (and updated if applicable) at least once a year.

The relationship with most service users is likely to last less than a year. In these cases, there is no need to conduct any annual pro-active checks for correctness.

Pro-actively checking employee Personal Data is not practical where the employee has left the business.

More frequent update checks are encouraged and can be integrated into other activities, such as account management calls made to service users, or ad-hoc checks made from time to time.

When Personal Data is checked for correctness, a record should be made of:

- The date the Personal Data was checked.
- Whether any corrections were necessary.
- Where corrections were collected directly from the person described by it, their name.

These records should be:

- Attached to the relevant CRM record for service users and prospective service users.
- Stored in an employee's HR file, where employee Personal Data is collected.
- Kept with supplier records, in the case where supplier contact Personal Data has been acquired.

Secure Deletion of Personal Data

Personal Data must be deleted when its retention period has been reached, the GDPR's Right to erasure has been invoked, or it is otherwise no longer needed.

Copies of Personal Data held in physical or hardcopy format should be shredded or processed by a secure document destruction service when they need to be deleted.

Individual electronic copies of Personal Data held in files on PC or server storage should be shredded with file shredding software before they are deleted.

Where electronic copies are kept on a cloud-based service, undertakings should be secured from the service provider that the physical disks used in their infrastructure are securely destroyed at the end of their operational lives.

When Personal Data has been securely deleted, a record should be made of:

- The date the Personal Data was deleted.
- The type (ie. personal email address) and category of the deleted Personal Data.

These records should be stored in a single, central register.

If the Right to erasure is invoked by a data subject, it is permissible to retain a portion of their Personal Data. Such circumstances will apply when some Personal Data needs to be kept, for example:

- For record-keeping purposes in support of a legal obligation (e.g. payroll, sales invoices etc).
- To guarantee the rights of the data subject elsewhere under the GDPR or PECR (e.g. retaining an email address, telephone number or postal address on the suppression list used by the business).

The key point when retaining some Personal Data to fulfil a legal obligation (elsewhere in the GDPR or other legislation), is that the bare minimum information required is retained; and not used for any purpose other than meeting the legal obligation for which it is required.

Overseas safeguards

The following safeguards are in place when overseas data processors are used:

- Only use data processors based in the EU or the USA.
- Prefer use of EU-based data processors where practical.
- Only use US data processors who are Privacy Shield certified or have adopted EU Model Clauses.

Call recording

Where inbound and outbound voice or video-conference calls are recorded, this practice should be announced to all participants at (or before) the start of the call. Any participant who has not been provided with the appropriate Privacy Notice (for their role in the conversation) should be sent or otherwise given the opportunity to access the relevant Privacy Notice.

GPS tracking

Each vehicle provided by Kickstart is equipped with a GPS tracking device. Use of the GPS monitoring system allows the location of each vehicle in the fleet (and potentially its user) to be tracked.

The current location, or location history, of a vehicle should only be accessed in the GPS monitoring system under the following circumstances:

- When there is a valid reason for doing so (such as a vehicle being reported lost or stolen).
- When authorised by a senior manager

Each time the current location, or location history, of a vehicle is viewed in the GPS monitoring system, a record should be kept of:

- The date and time when the location/location history was viewed.
- The vehicle's registration.
- The name of the person who viewed the location/location history.
- The reason for viewing the location/location history.
- The name of the senior manager who gave authorised.
- Details on the parties (police, insurers etc) to whom the location or location history was shared with.

Disclosure of Personal Data

Personal Data must only be disclosed to recipients described in this policy.

Physical security measures for Personal Data

Any Personal Data that is held in physical or hardcopy form must be protected with appropriate security measures, such as a locked filing cabinet, safe or secure room.

Sensitive Personal Data should be stored separately and secured with additional physical security measures above and beyond other Personal Data in hardcopy form.

The policies of the business in other areas, including Information Security, also apply.

Technical security measures for Personal Data

Personal Data held in electronic form must also be protected with appropriate security measures.

As a minimum, all Personal Data held electronically must be encrypted when at rest in data storage systems. It must also be encrypted when being transmitted or otherwise distributed or transferred.

Personal Data must never be sent by email unless the message is encrypted. This includes email messages sent from one member of the business to another.

Sensitive Personal Data must be stored separately and secured with additional technical security measures (such as two-factor authentication).

Personal Data (including Sensitive Personal Data) must never be transferred on a portable storage device or other portable piece of hardware unless the information has been encrypted.

The policies of the business in other areas, including Information Security, also apply.

Data breaches

Data breaches range from smaller events, such as losing a piece of paper with someone's name and email address printed on it, to large-scale loss or theft of thousands of customer email addresses and telephone numbers.

Permanent loss of data resulting from backup failure, accidental erasure and corruption are also classed as data breaches.

The definition of a data breach also covers temporary loss of access to Personal Data, for example, due to service unavailability.

Assessing the risk posed by a data breach

The rights and freedoms of data subjects (people) may be affected by a data breach which:

- Puts them at risk of discrimination
- Leads the theft of their identity or other fraud
- Causes them financial loss
- Damages their reputation

Assessing the risk posed to data subjects from a data breach involves consideration of the following factors:

- The nature of the breach
- The type, sensitivity and volume of Personal Data affected
- How easy it is to identify the data subjects from the Personal Data in the breach
- How severe the consequences could be for the affected data subjects
- Any special characteristics possessed by the data subjects (e.g. a breach involving the loss of home addresses for children is more severe than a breach where the business addresses of adults were lost)
- The number of data subjects affected by the breach
- Any special characteristics possessed by the organisation who has suffered the breach (e.g. a hospital losing medical records is more severe than a marketing agency losing a list of business postal addresses)

If a significant risk is posed to the rights and freedoms of any single data subject, it is mandatory to report the breach to the ICO.

Recording a data breach

All data breaches must be recorded, with following details captured:

- Date and time the breach occurred
- Date and time the breach was discovered
- How the breach was detected
- Details of the risk assessment that was performed to ascertain whether a risk to a data subject's rights and freedoms resulted from the breach.
- What measures have been taken to guarantee the rights of the data subjects whose Personal Data was accessed, lost or stolen in the breach.

- What measures have been put in place to prevent a similar breach in the future.
- Whether the breach was reported to the ICO – and if so – the date and time this was done.

Reporting a data breach to the ICO

It is mandatory to report a data breach to the ICO if it is likely to result in a risk to someone's (whose Personal Data is being processed) rights and freedoms.

Where applicable, a data breach must be reported to the ICO as soon as is feasibly possible and, at the latest, within 72 hours of the breach occurring.

Data processors and data breaches

Contractual and operational measures must be in place with all data processors used, that compel them to promptly notify the business if they suffer a data breach.

While data processors also have obligations in law concerning data breaches, the prime responsibility for risk assessment and reporting to the ICO lies with the business.

Documentation

As a company of fewer than 250 people, the business is only obliged to document frequent ("not occasional") Personal Data processing activity.

Frequent processing activity is defined by this policy as operations concerning one or more of the following:

- Employee recruitment
- Employee management and support
- Marketing to prospective service users
- Marketing to existing service users
- Selling to prospective service users
- Selling (including account management) to existing service users

In all cases, referenced document sets must be kept current and up-to-date, with an archive of prior versions retained for future reference.

Processing Purposes

The purposes for which Personal Data are processed are documented in this policy and the suite of Privacy Notices used by the business.

Data Sharing

The recipients with whom Personal Data is shared are described in this policy and the suite of Privacy Notices used by the business.

Retention

The retention policies applied to Personal Data processed by the business are described in this policy and the suite of Privacy Notices used by the business.

Information required for Privacy Notices

Privacy Notices are formed on the basis of the Legitimate Interest Test suite held by the business, this policy, employment contracts held by the HR Department, alongside service user and supplier contracts held by the Finance Department.

Records of consent

Consent is recorded and tracked in the CRM system used by the business and the suppression list it maintains. Consent records for data subjects included on purchased marketing lists are held by the Marketing Department.

Controller-processor contracts

Copies of these contracts are retained by the Finance Department.

Location of personal data

Each location where the business stores Personal Data is described in the external Personal Data Mapping document.

Data Protection Impact Assessment (DPIA) reports

Copies of these reports are held by the Operations Department.

Records of Personal Data Breaches

These records, produced in accordance with this policy, are held by the Operations Department.

Technical and Organisational security measures

The security measures applied to Personal Data are described in this policy, the Information Security policy observed by the business, operational processes the business has in place and other relevant policies (e.g. clear desk policy).

Other records

Records concerning:

- Documented sources of Personal Data
- Personal Data updates
- Secure deletion of Personal Data

should also be kept, as described elsewhere in this policy.

Personal Data Taxonomy

The Employee Personal Data Purposes Table should be read in conjunction with this taxonomy.

Processed with consent

Purpose	Personal Data collected	Categories	Data Subject	Recipients	Retention	Overseas
Employee biographies for marketing	Name Photo Professional experience summary	Identity Professional experience	Employee	N/A	Until employee leaves the business	N/A
Verifying that employees hold a valid driving licence	Driving Licence Details (including any convictions)	Driving Licence Criminal Convictions	Employee	N/A	While employed and with access to a company vehicle	N/A
Background check results	Criminal Conviction Details (if applicable)	Criminal Convictions	Employee	N/A	Up to 6 months after background checks completed	N/A
Understanding fitness to work following an examination by a company doctor	Health Details	Health	Employee	N/A	Up to 6 months after the employee has left the business	N/A
Arranging insurance under fleet policy	Driving Licence Convictions Criminal Conviction Details Health Details	Criminal Convictions Health	Service user	<insurer>	Up to 3 months after hire has concluded	N/A
Diversity and inclusion monitoring	Ethnic origin Disability status	Ethnicity Disability	Service user	n/a	Up to 3 months after hire has concluded	N/A

Processed to support entry to or the performance of a contract

Purpose	Personal Data collected	Categories	Data Subject	Contract	Recipients	Retention	Overseas
Contacting service users to discuss on-going hire	Contact Details	Contact Details	Service User	Hire	N/A	Up to 3 months after hire has concluded	N/A
Arranging insurance under fleet policy	Motoring Accident Details Motoring Insurance Details	Motoring Accident Motoring Insurance	Service User	Hire	<insurer>	Up to 3 months after hire has concluded	N/A
Arranging the hire of a vehicle	Name Address Tenancy Details Date of Birth Contact Telephone Numbers Driving Licence Details Employer/equivalent Details Social Worker Details UK Residency Hire Details	Contact Details Tenancy Date of Birth Driving Licence Employment/Training Social Worker Residency Hire Details	Service User	Hire	n/a	Up to 3 months after start of hire	N/A
Hiring out a vehicle	Name Address Date of Birth Contact Telephone Numbers Driving Licence Details Hire Details	Contact Details Tenancy Date of Birth Driving Licence Hire Details	Service User	Hire	n/a	Up to 3 months after conclusion of hire	N/A
Summarising service use	Tenancy Details Date of Birth Employment Status Social Worker Details UK Residency	Tenancy Date of Birth Employment/Training Social Worker Residency	Service User	Hire	Anonymised before sharing summaries	Up to 3 months after hire has concluded	N/A
Tracking vehicle location	Vehicle Details	Vehicle	Service User	Hire	Police Insurers	Up to 3 months after hire has concluded	N/A
Taking up references	Referee Details	Personal Referees	Service User Referees	Hire	n/a	Up to 3 months after start of hire	N/A

In all cases, if an employee is unprepared or unwilling to provide the Personal Data require to support the entry to the employment contract, or the performance of it, this will call into the question whether the contract can proceed.

Processed to comply with a legal obligation

Purpose	Personal Data collected	Categories	Data Subject	Legal Obligation(s)	Recipients	Retention	Overseas
Maintaining visitor records to comply with fire regulations	Name Employer Name Vehicle Registration	Identity Employment Vehicle	Visitor	Fire regulations	N/A	3 months after visit to office	N/A
Hire record-keeping to meet HMRC obligations	Name Address	Contact Details	Service User	Taxation	HMRC	7 years after conclusion of hire	N/A
Diversity and equality monitoring	Ethnic origin Disability status	Ethnicity Disability	Employee	Equalities Act	N/A	Up to 6 months after employee departure	N/A
Officeholder record-keeping	Name Address Profession	Contact Details Professional Details	Officeholder	Companies Act	Companies House HMRC	7 years after association with the company ceases	N/A
Verifying identity of Data Subjects using their rights	Name Proof of Identity	Identity	Employee Service User Visitor Supplier Referees Officeholders	Data Protection	n/a	Until identity verified	N/A
Guaranteeing Data Subjects' rights	Name Copy Correspondence	Identity Correspondence	Employee Service User Visitor Supplier Referees Officeholders	Data Protection	n/a	3 years after request handled	N/A
Right of erasure record-keeping	Name	Identity	Employee Service User Visitor Supplier Referees	Data Protection	n/a	3 years after request agreed	N/A
Suppression list record-keeping	Name Email Address Telephone Numbers Address Social Media Handles	Contact Details	Service User	Data Protection	n/a	Indefinitely	N/A

In all cases, if an employee is unprepared or unwilling to provide the Personal Data required to support the business in discharging its legal obligations, their employment contract cannot be executed.

Should any visitors to the business refuse to provide their Personal Data required to aid the business in complying with fire regulations, they will be refused entry to the premises and asked to leave the site.

Processed in a legitimate interest

Purpose	Personal Data collected	Categories	Data Subject	Legitimate interests	Recipients	Retention	Overseas
Establishing the good character of employees	Personal referee details	Name Contact Details	Employee Referee	Verifying employee character	N/A	Completion of probation; or 6 months after departure	N/A
Establishing the good character of employees	Personal references	Employee Character	Employee	Verifying employee character	N/A	Completion of probation; or 6 months after departure	N/A
Duty of care to employees	Next of kin details	Name Contact Details Address Details	Employee Next of kin	Duty of care	Emergency Services	Until departure	N/A
Validating employee work history	Professional referee details	Name Contact Details	Employee Referee	Validating employment history	N/A	Until departure; or 6 months after departure if probation not completed	N/A
Validating employee work history	Professional references	Employee Experience	Employee	Validating employment history	N/A	Completion of probation; or 6 months after departure	N/A
Providing access to employee benefits for dependents/partners	Name Address Contact Number Email Address	Contact Details	Dependent/Partner	Dependent/partner details required for their access to employee benefits	Benefits Provider	Until departure of employee from the business	N/A
Recruitment	Name Home Telephone Number Mobile Telephone Number Personal Email Address LinkedIn Profile Handle CV or employment profile Interview and/or assessment notes	Name Contact Details Professional Experience Recruitment Assessment	Prospective Employee	Recruiting employees whose skills are required by the business	N/A	6 months after application deemed unsuccessful; or 6 months after employment start date	N/A
Supplier retention and management	Name Job Title	Contact Details Correspondence	Supplier	Arranging the supply of products or	N/A	1 year after contact's	N/A

	Employing Organisation Address Mobile Telephone Office Telephone Number Email Address Copy Correspondence			services, and the on-going management of such arrangements		organisation ceases to supply the business, or alternative contact nominated	
Publishing company website	Visitor IP address Cookies sent with web requests	Website Visitor	Website Visitor	- Monitoring and improving our website and services - Protection and assertion of legal rights - Protection of the business against risks	N/A	3 months after website visit	N/A
Customer feedback	Name Mobile Telephone Number Customer Feedback Details	Contact Details Account Details Customer Feedback	Customer	Soliciting customer feedback on the customer service they experience	N/A	1 year after contact's organisation is no longer a customer	N/A
Customer testimonials	Name Area	Contact Details	Customer	Soliciting and publishing customer testimonials concerning the products and services offered by the business	Made Public	Until opt-out used	N/A
Arranging AGMs, EGMs etc	Name Address Contact Telephone Numbers Email Address	Contact Details	Officeholder	Managing events and activities relevant to officeholders of the company	N/A	Retained for this purpose while actively associated with the company	N/A
Taking up pre-hire personal references	Personal Referee Details	Name Contact Details	Service User Referee	Establishing the good character of prospective service users	N/A	3 months after start of hire; or 6 months otherwise	N/A