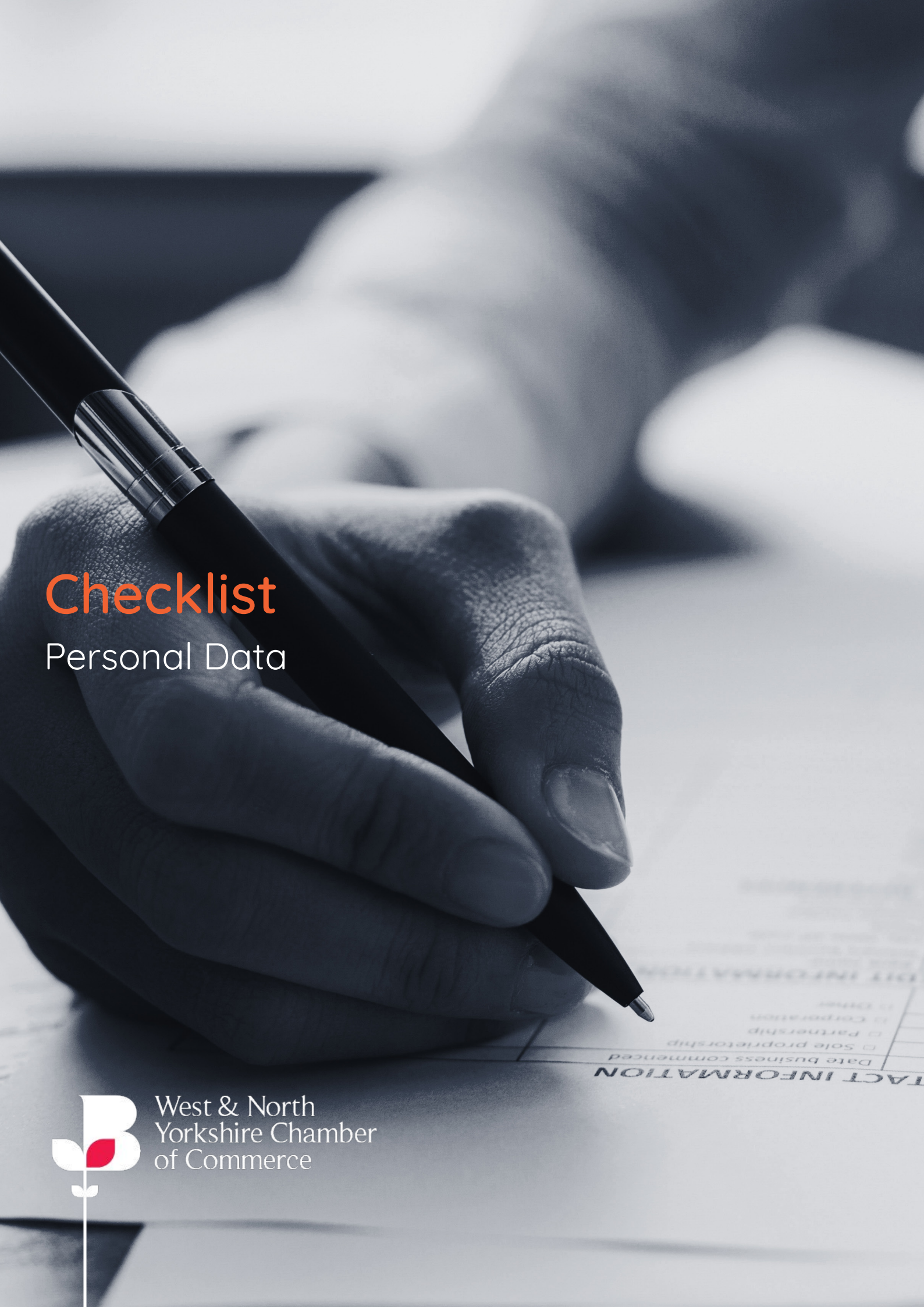

Checklist

Personal Data

West & North Yorkshire Chamber of Commerce

General Data Protection Regulations

On 25 May 2018 the General Data Protection Regulations take effect. This will have a significant impact on every business within the United Kingdom. It is important to take steps now before implementation so you are ready.

GDPR will affect you in a number of ways:

HR perspective

- Employing staff, permanent, temporary or contractors

Business perspective:

- Operating as a Business to Business (B2B) or Business to consumer (B2C)

Where you process personal data you will need:

- Privacy notice/standard relating to staff/customers
- GDPR policy
- Where you outsource data - a contract with third parties
- Where you process special data - documentation/record of your activities to demonstrate you are complying

Definitions

Data controller
The person or organisation who determines the purpose and means of processing personal data

Processor
Someone who is responsible for processing personal data on behalf of the data controller

Personal data
Under the Regulations the definitions have been widened to include all kinds of personal data. Personal data is defined as "any information relating to a data subject". This includes any expression of an opinion. A data subject is the identified or identifiable natural person to whom personal data relates. e.g. a data subject is an employee, contractor but this could also be a customer.

The definition includes data where you can identify an individual via their: personal email address, data for logging onto a computer, CCTV etc. Customer email address; bank details home address etc.

Special data – what is it?

Special data that reveal:

- Racial or ethnic origin;
- Political opinions;
- Religious and philosophical beliefs;
- Trade Union membership;
- Genetic data;
- Biometric data for uniquely identifying a natural person; and
- Sex life and sexual orientation.

The journey of data

If you have any data which falls within the definition of Personal data and you do any one of the following activities this is known as "**Processing**".

- Collecting
- Recording
- Organising
- Structuring

- Storing
- Adapting or altering
- Retrieving
- Consulting
- Using
- Disclosure by transmission
- Dissemination or otherwise making available
- Alignment or combination
- Restriction (that is, the marking of stored data with the aim of limiting its processing in the future)
- Erasing
- Destruction

Just doing nothing with personal data is still processing.

Business to Business

- In a business to business context you will have data regarding employees/temporary staff/ contractors but your customer base will be companies rather than individuals.
- In this scenario GPDR will apply to your staff but there are occasions where you will have data about customers of those companies where they are individuals.

Examples

- A Company manufacturer makes goods to another business, you may also come into possession of that business customer`s details. If they are a person then you will be caught under the GDPR.
- A designer has made some windows for a fitting company only to receive the consumer details of who they are and their address.
- The advice here is to thoroughly carry out an audit of your Customers and all the data you hold.

Business to Consumer

- Where you operate business to consumer then you will be caught under the GDPR, because you will have your consumer's details, as well as the HR data eg
- Name, address, email address, etc delivery information.

What do I need to do to comply with the GDPR?

- Carry out a thorough audit
- Attached is a template to help you identify what type of personal data you are holding in respect of an employee and customers etc.
- Consider: Where is the data coming from, where is it being stored who as access and where is it going to?

In using the template think about the following:

- The business's personal data processing activities, such as how the business collects, uses, shares, and otherwise processes personal data;
- The different types of personal data involved in those processing activities;
- The different types of data subjects and where they reside;
- Why the business engages in the processing activity;
- The parties who may access the personal data, such as data processors and other third parties, and the types of personal data disclosed;
- The different business systems that store or process personal data, including electronic databases and the people responsible for those systems;
- The geographic locations where the business stores personal data;
- The electronic personal data flows, including data transfer, sharing, storage, exit, and destruction points;
- How long the business retains personal data; and
- The security controls and safeguards deployed to protect personal data.

Where is the data being stored?

- Operations;
- Human resources;
- Records and information management;
- Information technology, iCloud, iPhones
- Marketing;
- Finance;
- Webpage design;

- Product development;
- Externally

Having completed an audit what do I do next?

Once you have carried out an audit the next step is to consider whether you are complying with the GDPR principles in order for you to process this data lawfully.

Step 1 – The Principles:

The GDPR sets out a number of principles with which data controllers and processors must comply when processing personal data. These principles form the core of the obligations of the data controller and will usually form the basis of any claim that a data controller has not complied with its statutory duties.

A data controller is the person or organisation that determines when and how to process personal data – this tends to be in the name of the business.

The Data Processor is the person processing the data.

The Principles are:

a. Processed lawfully, fairly and in a transparent manner in relation to individuals;
b. 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;
c. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
d. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;
e. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 the GDPR in order to safeguard the rights and freedoms of individuals; and
f. 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."

Not only do you have to satisfy the Principles but also whether you are processing the data lawfully.

Step 2 Identify the lawful basis of processing

To process data you must have a valid lawful basis.
Where you are processing special data then you need to satisfy a special condition (step 3).
For the moment looking at ordinary general data you need to identify a lawful process.

Lawful basis for processing

At least one of these must apply whenever you process personal data. This must be determined before you begin processing. There may be more than one. Select the one which is appropriate to the activity you are doing:

a. Consent: the individual has given clear consent for you to process their personal data for a specific purpose. Consent requires a positive opt-in. Don't use pre-ticked boxes or any other method of default consent. Explicit consent requires a very clear and specific statement of consent.
b. Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
c. Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
d. Vital interests: the processing is necessary to protect someone's life.
e. Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
f. Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Step 3 Special data and conditions

Special data is personal data that reveals:

- Racial or ethnic origin;
- Political opinions;
- Religious and philosophical beliefs;
- Trade Union membership
- Biometric data for uniquely identifying a natural person; and
- Sex life and sexual orientation.

In order to lawfully process special category data, you must identify both a lawful basis and a separate condition. These do not have to be linked.

Special data conditions

The conditions to be applied are:

- The data subject has provided explicit consent

The processing is necessary for:

- Carrying out the data controller's rights in the field of employment law, social security, and social protection;
- Protecting the vital interests of the data subject when the data controller cannot obtain consent;
- Establishing, exercising, or defending legal claims;
- Reasons of substantial public interest;
- Purposes of preventive or occupational medicine to assess the working capacity of a data subject, medical diagnosis, or for the provision of health or social care or treatment;
- Reasons of public interest in the area of public health;
- Archiving in the public interest; or
- Scientific, historical research, or statistical purposes.
- The processing relates to the legitimate activities of certain non-profit organisations.
- The processing relates to personal data made public by the data subject.

Privacy notices/standard

- The GDPR sets out information which you are obliged to inform those of how you will use personal and sensitive data. This is called a "fair processing notice" also known as a "Privacy Notice/Standard"
- You can use this notice to notify employees, workers and contractors customers about the personal data that you hold relating to them, how they can expect their personal data to be used and for what purposes. i.e your intended purpose for processing the personal data and the lawful basis for the processing.

Individual rights

Under GDPR Individuals have the right to:

1. Have access to their personal data
2. The right to rectification. The GDPR gives individuals the right to have personal data rectified. Personal data can be rectified if it is inaccurate or incomplete.
3. The right to erase – the right to be forgotten
4. The right to restrict processing, individuals have a right to 'block' or suppress processing of personal data.
5. The right to data portability - the right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
6. The right to object processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.
7. Rights in relation to automated decision making and profiling automated individual decision-making (making a decision solely by automated means without any profiling can be part of an automated decision-making process, human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual).

Accountability

You are expected to put into place measures/tools to show compliance.

You must:

- Implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include:
- Internal data protection policies such as staff training, internal audits of processing activities,
- Reviews of internal HR policies; maintain relevant documentation on processing activities;
- Where appropriate appoint a data protection officer; implement measures that meet the principles of data protection by design and data protection by default. Measures could include: data minimisation; pseudonymisation;
- Transparency; allowing individuals to monitor processing; and creating and improving security features on an ongoing basis.
- Use data protection impact assessments where appropriate

Contracts

- Whenever a controller uses an external processor it needs to have a written contract in place. The contract is important so that both parties understand their responsibilities and liabilities.
- Eg payroll/ IT/HR
- The GDPR sets out what needs to be included in the contract. These contracts must now include certain specific terms, as a minimum.

Documenting your processing activities

- That the GDPR contains explicit provisions about documenting your processing activities.
- The ICO guidance states that:
- The GDPR contains explicit provisions about documenting your processing activities.
- You must maintain records on several things such as processing purposes, data sharing and retention.
- You may be required to make the records available to the ICO on request.
- Documentation can help you comply with other aspects of the GDPR and improve your data governance.
- Controllers and processors both have documentation obligations.
- For small and medium-sized organisations, documentation requirements are limited to certain types of processing activities.
- Information audits or data-mapping exercises can feed into the documentation of your processing activities.
- Records must be kept in writing.
- Most organisations will benefit from maintaining their records electronically. Records must be kept up to date and reflect your current processing activities.

Breaches

- Access by an unauthorised party
- Sending personal data to an incorrect recipient – email
- Losing data
- Altering without permission
- You must keep a record of all breaches regardless of the severity
- Where a breach is of high risk of adversely affecting individuals you must report to the ICO within 72 hours of being aware of the breach and inform those affected

Cases

Just Eat:

- A customer's phone number is used for reasons for which it was not originally taken, it could be a breach of the Data Protection Act.
- "Organisations have a legal duty to make sure personal data is only used for the purposes for which it was obtained. We are aware of reports of an incident involving Just Eat and will be looking into it."
- A firm of loss adjusters has been fined £50,000 for unlawfully disclosing personal data which had been obtained illegally by senior employees,
- ICO have secured eight convictions against NHS employees who were caught prying into the medical records of patients, friends, colleagues or other people they knew without a valid or legal reason.e private investigators.
- There were eight convictions in 2017 attracted fines and costs totalling more than £8,000 – but in the future, we would like to see custodial sentences introduced as a sentencing option for the courts in the most serious cases.
- People working with personal information have been warned they have to obey strict privacy laws after a charity worker was prosecuted for making his own copies of sensitive data.
- Robert Morrisey, 63, sent spreadsheets containing the information of vulnerable clients to his personal email address without the knowledge of the data controller, his employer the Rochdale Connections Trust.
- The defendant sent 11 emails from his work email account on 22 February 2017, which contained the sensitive personal data of 183 people, three of whom were children. The personal data included full names, dates of birth, telephone numbers and medical information. Further investigation showed that he had sent a similar database to his personal account on 14 June 2016.
- Morrisey, of Milnrow, Rochdale, appeared at Preston Crown Court and admitted unlawfully obtaining personal data in breach of Section 55 of the Data Protection Act 1998. He was given a conditional discharge for two years and was also ordered to pay prosecution costs of £1,845.25, as well as a victim surcharge of £15.

Checklist – Personal Data Template 1

What personal data are you holding about an employee or customer?

Does it include some or all of the following Data?

What will you do with this data?

Types of Data	Where did the data come from?	What are we using it for/the purpose?	Who will have access/use of the data internal external?	Where is this being stored/ held?	What is the lawful basis for processing?	How long are we keeping it for?
Personal contact details such as: name, title, addresses, telephone numbers, personal email addresses						
Date of birth						
Gender						
Marital status and dependants						
Next of kin and emergency contact information						
Government identification numbers such as national insurance number, driver's licence number or other identification card number						
Bank account details and payroll information						

Salary, annual leave and benefit information.						
Compensation history						
Performance information						
Disciplinary and grievance information, where applicable						
Pension and insurance enrolment information						
Start date and job title						
Location of employment						
Education and training						
Employment records (including professional memberships, references, work history, and proof of work eligibility)						
Photograph						
Other personal details included in a CV or cover letter or that the employee has otherwise voluntarily provided						