
BHConsulting

Who am I?

- COO, BH Consulting
- Previously CISO, KBC Bank Dublin x 15years
- Almost 30 years working in ICT
- Academic:
  - *(Currently) PhD In Information Privacy Protection, DCU*
  - *Masters in Business and Leadership, UCC*
  - *BSc in Information Systems (Hons), TCD*
  - *Chartered InfoSec Professional (CISSP) since 2001*
  - *Post Grad Diploma in Executive Coaching, UCC*
  - *Post Grad Diploma in Cloud Computing Strategy, UCC*
  - *Diploma in Systems Analysis, TCD*
  - *Diploma in Web Design*

BH Consulting

RECAP OF KEY GDPR FEATURES

ITS NOT ABOUT THE DATA!!

What the new EU GDPR means in 1 minute

The EU GDPR will increase privacy for individuals and give regulatory authorities greater powers to take action against businesses that breach the new laws. Here's what it means for your business:

Tough penalties: fines of up to

4% of annual global revenue

or

€20 million, whichever is greater.

The regulation also applies to **non-EU companies** that process personal data of individuals in the EU.

The **international transfer of data** will continue to be governed under EU GDPR rules.

The **definition of personal data** is now broader and includes identifiers such as

genetic

mental

cultural

economic

social identity.

Obtaining consent for processing personal data must be clear, and must seek an affirmative response.

Parental consent is required for the processing of **personal data of children** under age 16.

Data subjects have the **right to be forgotten** and erased from records.

Users may request a copy of personal **data in a portable format**.

The appointment of a **data protection officer** (DPO) will be mandatory for companies processing high volumes of personal data and good practice for others.

Privacy risk impact assessments will be required for projects where privacy risks are high.

Controllers must **report a data breach** no later than

72 hours

after becoming aware of the breach, unless the breach has a low risk to the individual's rights.

Products, systems and processes must consider **privacy-by-design** concepts during development.

Data controllers must ensure adequate contracts are in place to **govern data processors**.

Data processors can be held **directly liable** for the security of personal data.

Controllers must have a **legal basis for processing** and collecting personal data.

One-stop shop: international companies will only have to deal with one supervisory data protection authority.

ISO 27001 and other certifications will help demonstrate "**adequate technical and organisational measures**" to protect persons' data and systems.

You have to comply with EU GDPR by MAY 2018

What it Means to The Individual

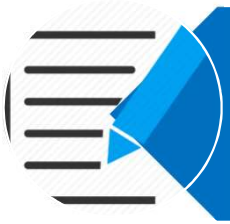
Stricter rules for obtaining consent as a legal basis for processing.

Consent can be withdrawn at any time

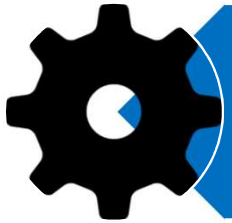
Right to be forgotten and have personal data erased

Right to clear information relating to the scope, purpose and retention of personal data

Data portability – right to move personal data to another provider



Right to rectify inaccurate data



Automated processing – right not to be subject to an automated decision

Subject access requests - right to obtain a copy of their personal data

Right to make a compensation claim for damages suffered

What it Means to Organisations?

Conduct a privacy risk assessment of how all personal data is collected, used, stored, and accessed throughout the organisation

Data Security - keep personal data secure through appropriate technical and organisational measures

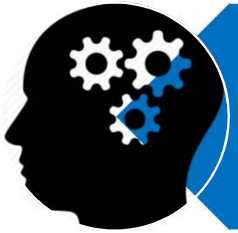
Demonstrate accountability and compliance to the GPDR by maintaining documentary evidence of all data processing activities

Data Breaches – report data breaches to the regulator within 72 hours

Where personal data is transferred outside of the EU? You must demonstrate the adequacy of the safeguards in place

Consider the data protection role within
the organisation

A full audit of supply chain is required. Verify that adequate data protection safeguards are in place with suppliers who process personal data



Demonstrate that privacy by design is built into technical solutions and organisational practices

What it Means to Organisations?

Fines of up to 1 Million for Public Bodies

Compensation claims for damages suffered

Possible prison sentences for deliberately breaching the GDPR

Reputational damage to the brand and loss of customer trust

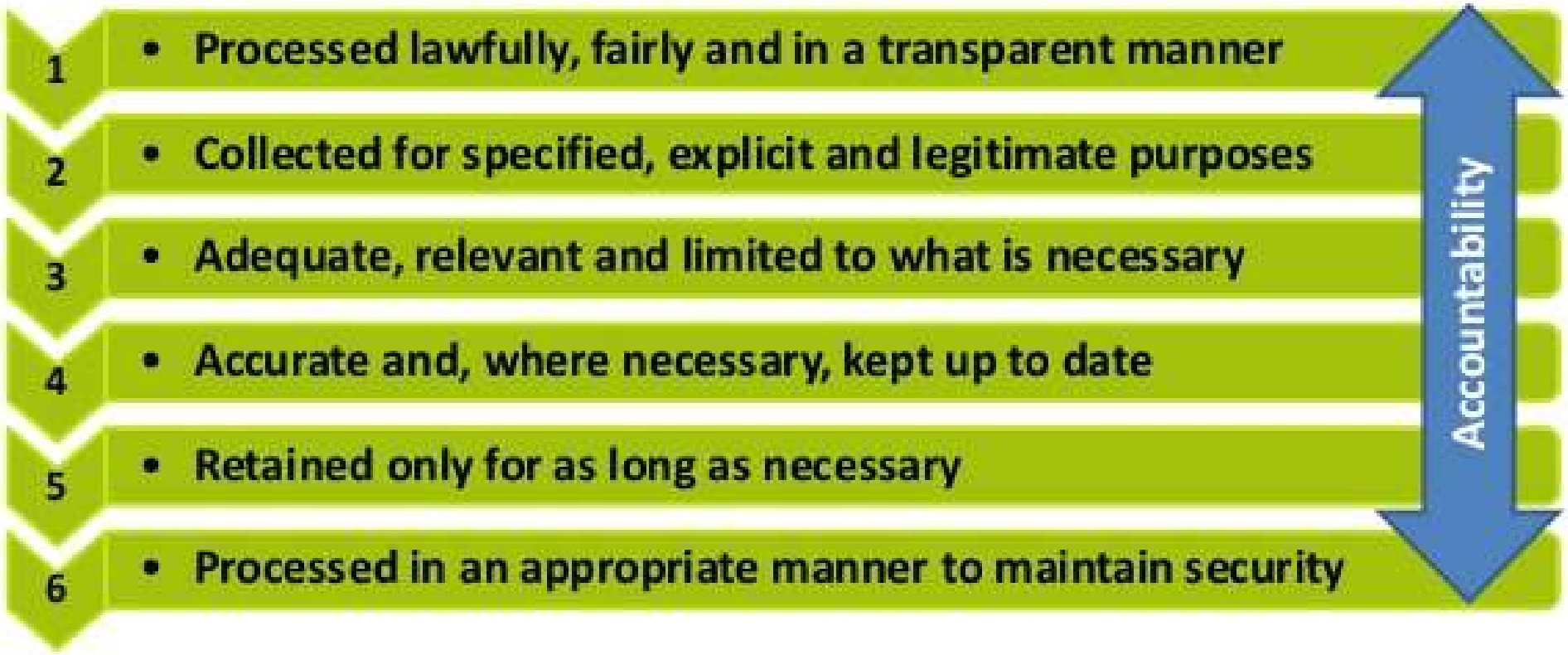
BHConsulting

Accountability Principle

BHConsulting

The Principle of Accountability and What It Means:

- Article 5: *Principles relating to processing of personal data*
- "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability'). "



ACCOUNTABILITY CHECKLIST

We take responsibility for complying with the GDPR, at the highest management level and throughout our organisation as demonstrated:

☐ We keep evidence of the steps we take to comply with the GDPR.
☐ We put in place appropriate technical and organisational measures, such as:
- ❑ adopting and implementing data protection policies (where proportionate);
- ❑ taking a 'data protection by design and default' approach - putting appropriate data protection measures in place throughout the lifecycle of our processing operations;
- ❑ putting contracts in place with organisations that process personal data on our behalf;
- ❑ maintaining documentation of our processing activities;
- ❑ implementing appropriate security measures;
- ❑ recording and, where necessary, reporting personal data breaches;
- ❑ carrying out DPIAs for uses of personal data likely to result in high risk to DS rights;
- ❑ appointing a data protection officer (where necessary); and
- ❑ adhering to relevant codes of conduct and signing up to certification schemes (where possible).

☐ We review and update our accountability measures at appropriate intervals.

BHConsulting

Exercise #1:

Who are the key GDPR stakeholders in FCC ?

BHConsulting

BHConsulting

BHConsulting

What is Sensitive Data?

- Racial, Ethnic origin
- Religious or philosophical beliefs
- Political opinions
- Trade union membership
- Genetic data
- Biometric data
- Health
- Sexual orientation

GREAT PLACE TO WORK®
WORLD'S BEST WORKPLACES™
2017

BH Consulting

QUIZ: PERSONAL OR SENSITIVE?

- **Org Name. Life Insurance Inc. *Email Address of customer***
- **Org Name: SIPTU. *Email address of member Name***
- **Org Name: Beaumont Mental Hospital. *Patient Name***
- **Chromosomal data belonging to Joe Bloggs**
- **Children's ages, dobs and schools.**
- **Children's health information**
- **Fitbit activity data belonging to Elmer Fudd**
- **Location data from Fitbit regarding Elmer Fudd**
- **HR Wellbeing Survey to employees – responses**

BHConsulting

BHConsulting

SOME IMPORTANT CAVEATS...

BHConsulting

Privacy Policies and Privacy Statements

Data and Cyber-Related Regulation

- 2017 – The NIS Directive
- 2018 – GDPR
- Local housing authority statutory instruments
- Coming….PECR (e-Privacy)
- The Health Information and Patient Safety Bill
- Consumer Protection Codes
- Child Protection
- Freedom of Information

GDPR LAWFULNESS PERSONAL DATA PROCESSING

Legal grounds and lawful basis - processing lawful if at least one of legal bases below

Consent

The consent of a data subject to the processing of his/her personal data

Legitimate interests

There is a weighed & balanced legitimate interest where processing is needed and the interest is not overridden by others

Public interest

Public authorities and organizations in the scope of public duties and interest

Contractual necessity

Processing is needed in order to enter into or perform a contract

Legal obligations

The controller is obliged to process personal data for a legal obligation

Vital interests

It is vital that specific data are processed for matters of life and death

Public Interest

A public authority should identify a clear 'legal' basis for the task, function or power that uses personal data.

What is the 'public task' basis?

Article 6(1)(e) gives you a lawful basis for processing where:

> "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller"

This can apply if you are either:

- carrying out a specific task in the public interest which is laid down by law; or
- exercising official authority (for example, a public body's tasks, functions, duties or powers) which is laid down by law.

If you can show you are exercising official authority, including use of discretionary powers, there is no additional public interest test. However, you must be able to demonstrate that the processing is 'necessary' for that purpose.

'Necessary' means that the processing must be a targeted and proportionate way of achieving your purpose. You do not have a lawful basis for processing if there is another reasonable and less intrusive way to achieve the same result.

Public Interest

The public interest legal basis will cover processing necessary for (not exhaustive):

- the administration of justice;
- parliamentary functions;
- statutory functions;
- governmental functions;
- activities that support or promote democratic engagement.

Consider an alternative lawful basis if you are not confident that processing is necessary for a relevant task, function or power which is clearly set out in law.

Remember that the GDPR specifically says that further processing for certain purposes should be considered to be compatible with your original purpose. This means that if you originally processed the personal data for a relevant task or function, you do not need a separate lawful basis for any further processing for:

- archiving purposes in the public interest;
- scientific research purposes; or
- statistical purposes.

BHConsulting

What is Consent?

- **Freely given, not coerced**
- **Specific**
- **Informed**
- **Unambiguous**
- **A demonstrated indication of agreement**
- **Can be withdrawn at any time**
- **Silence or inactivity <u>does not constitute, neither does it imply consent!</u>**

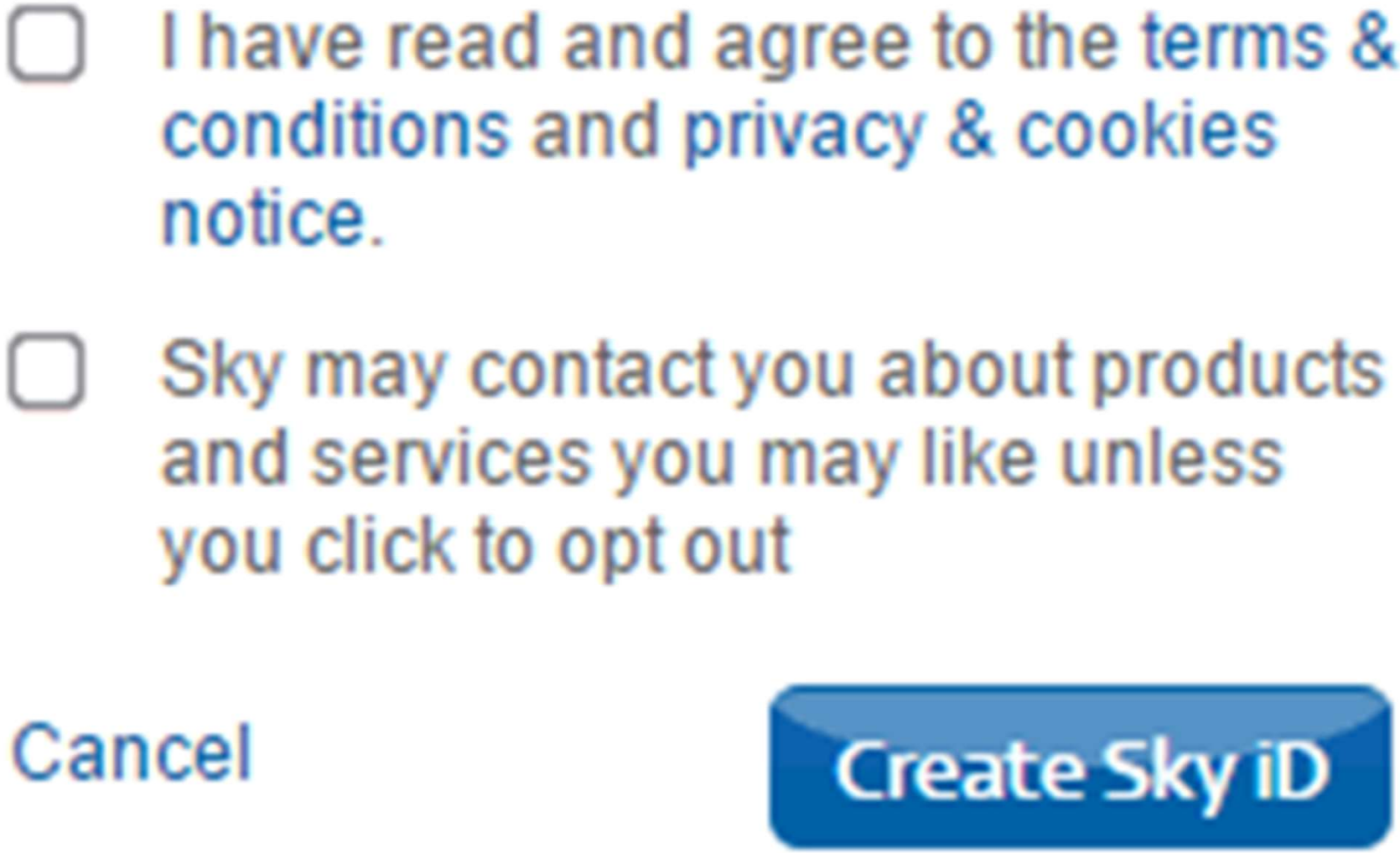
Example

I am happy for my personal data to be processed for the following purposes:

- ❑ to send me communications about the charity's events and activities (including fundraising)
- ❑ to share my details with [trading company]
- ❑ to share my details with [specify other arts organisations, by name, with which you may share data]

I am happy to receive communications about the charity's events and activities (including fundraising) by:

- ❑ phone
- ❑ email
- ❑ post

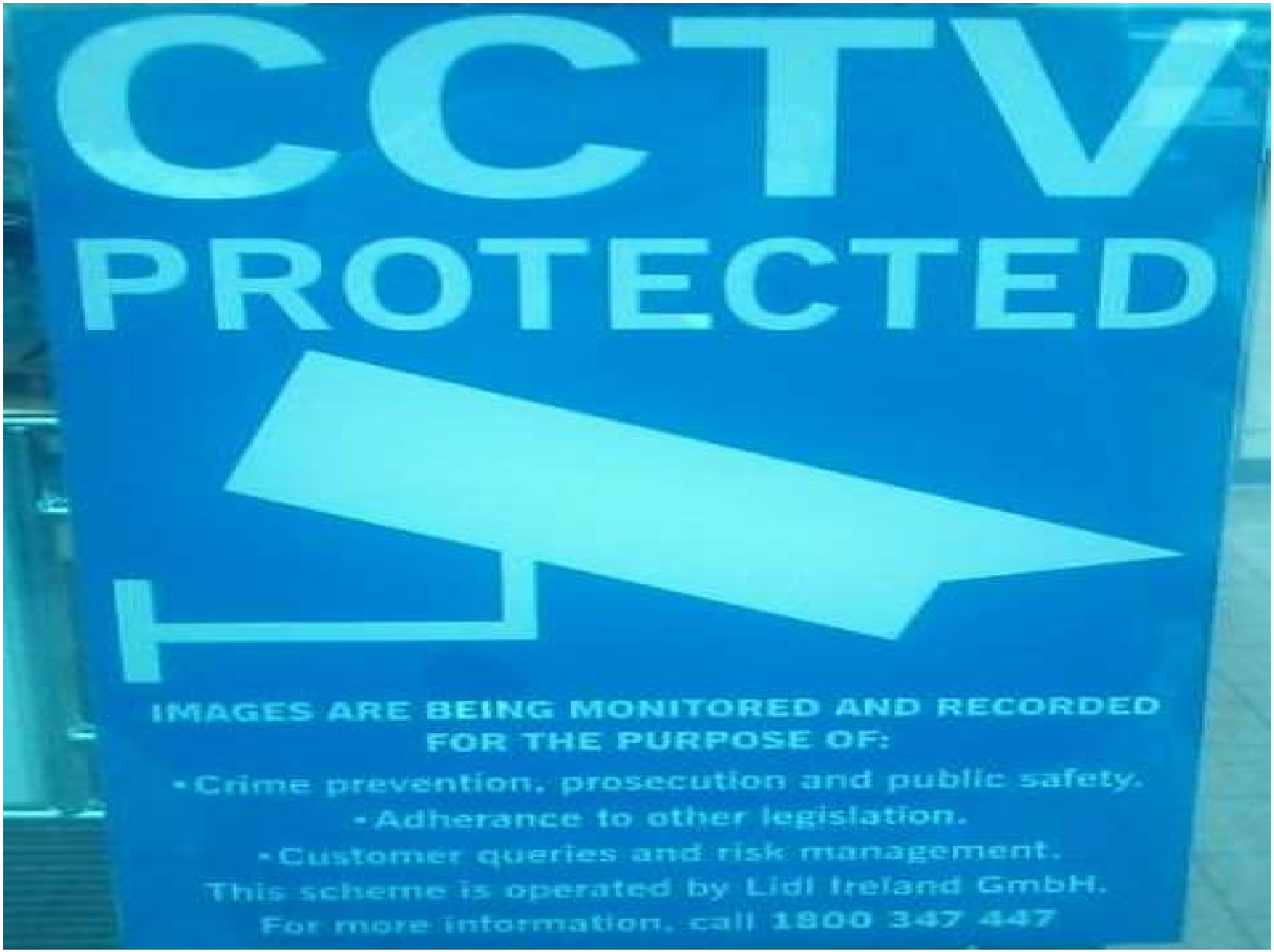

I have read and agree to the terms & conditions and privacy & cookies notice.
Sky may contact you about products and services you may like unless you click to opt out
Cancel
Create Sky iD

Updates from Twitter

Email me with

- [x] News about Twitter product and feature updates
- [x] Tips on getting more out of Twitter
- [x] Things I missed since I last logged into Twitter
- [x] News about Twitter on partner products and other third party services
- [x] Participation in Twitter research surveys
- [x] Suggestions for recommended accounts
- [x] Suggestions based on my recent follows
- [x] Tips on Twitter business products

Save changes


CCTV
PROTECTED
IMAGES ARE BEING MONITORED AND RECORDED
FOR THE PURPOSE OF:
• Crime prevention, prosecution and public safety.
• Adherance to other legislation.
• Customer queries and risk management.
This scheme is operated by Lidl Ireland GmbH.
For more information, call 1800 347 447

BH Consulting

Special Category Information

- If you are processing special category data you need to identify both a lawful basis for general processing and an additional condition for processing this type of data (Art 6, and Art 9). These do not have to be linked.
- If you are processing criminal conviction data or data about offences you need to identify both a lawful basis for general processing and an additional condition for processing this type of data.

Special Category Information : Additional Legal Basis [Art 9(2)]

(a) the DS has given explicit consent to the processing.
(b) processing is necessary for the obligations and rights of the DC or DS for employment and social security and social protection law.
(c) processing is necessary to protect the vital interests of the DS.
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim, and processing relates to the members/former members or to persons with regular contact and that the personal data are not disclosed outside that body without DS consent;
(e) processing relates to personal data which are manifestly made public by the DS;
(f) processing is necessary for legal claims or whenever courts are acting in their judicial capacity;
(g) processing is necessary for reasons of substantial public interest;
(h) processing is necessary for occupational medicine, the assessment of the working capacity of the employee, medical diagnosis, provision or management of health/socialcare systems and services;
(i) processing is necessary for reasons of public interest in public health e.g. threats to health or ensuring high standards of quality of health care and medicinal products/devices,;
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

BHConsulting

Group Exercise

There has been a breach!! An employees HR file has been found in the car park and contains details of their diabetes and included salary and some sick notes.

Write a 5-step process on what to do?

- Who will you tell?
- Special category information involved?
- Who will you notify formally?
- Do you have any forms?
- What process will you put in place?
- Do you tell the DPC or the DPO?

1.Data mapping/data inventories
2.Data retention

BHConsulting

Data Mapping

BH Consulting

WHY DO DATA MAPPING?

Article 30 of the GDPR (Records of processing activities) states that organisations must maintain 'a record' of processing activities under [their] responsibility to include:

a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
b) the purposes of the processing;
c) a description of the categories of data subjects and of the categories of personal data;
d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation
f) where possible, the envisaged time limits for erasure of the different categories of data;
g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).
[…]

The controller or the processor […] shall make the record available to the supervisory authority on request.

BHConsulting

WHEN TO DO DATA MAPPING?

A Data Mapping Exercise project would be a suitable course of action if you are unable to answer any of the key questions below:

- Do we know where our sensitive data assets are?
- Do we know what type of data assets we have?
- Do we know how sensitive and valuable our data assets are?
- Do we know which business processes handle and store our sensitive data?
- Are we managing the risks to personal data effectively in line with GDPR requirements?
- Are we able to effectively report on our level of compliance?

BHConsulting

DATA MAP SIMPLE MANTRA

1. Capture
2. Store
3. Share

WHEN?
WHY?
WHO?
FOR HOW LONG?

BHConsulting

HOW LONG FOR RETENTION?

QUESTIONS TO ASK BEFORE MAPPING?

1. Which departments within your organisation are most likely to have data?
2. Who within each department would you need to speak with to find out what data exists?
3. Is it more efficient to send the relevant people a questionnaire or to speak with them directly?
4. What is the best way to receive/sort information from each person that collects data?
5. How much time will it take to complete the data map?
6. What information should you consider including in your data map:

- The types of data collected.
- Where the data is physically housed (*e.g.,* the building or location) , where the data is logically housed (*e.g.,* the electronic location within a server).
- Whether encryption is applied to the data in transit (*e.g.,* when it is moving). If it is, what encryption standard is being used? At rest?
- The custodian of the data (*e.g.,* who is responsible for it).
- Who has access within the organisation to the data, and outside of the organisation.
- Whether the data crosses national boundaries.
- The retention schedule (if any) applied to the data.

BHConsulting

KEY ELEMENTS OF A DATA MAP?

A data map shows the flow of your organisation's data from one location to another, such as from different business units or suppliers through to customers.

Data mapping allows you to identify any unforeseen or unintended uses. It's useful for processes where there are many steps or parties involved and you want to ensure that you've identified all the components in that process.

The data mapping process establishes:

- The data items obtained (name, email, address, etc.);
- The format of the data (hard copy, digital copy, etc.);
- Transfer methods (internally or externally, post, telephone, etc.); and
- Where the data is stored (offices, the Cloud, third party, etc.)

BHConsulting

DATA MAPPING PROCESS CHALLENGES

Challenges in the data mapping process

Your DPO should play a key role in mapping the flow of information. Creating a data map can involve the following three challenges:

1.Identifying personal data (stored in what formats)

PD can include name, email address, identification number and location data. Personal data can be stored in a number of formats, including paper, digital or audio.

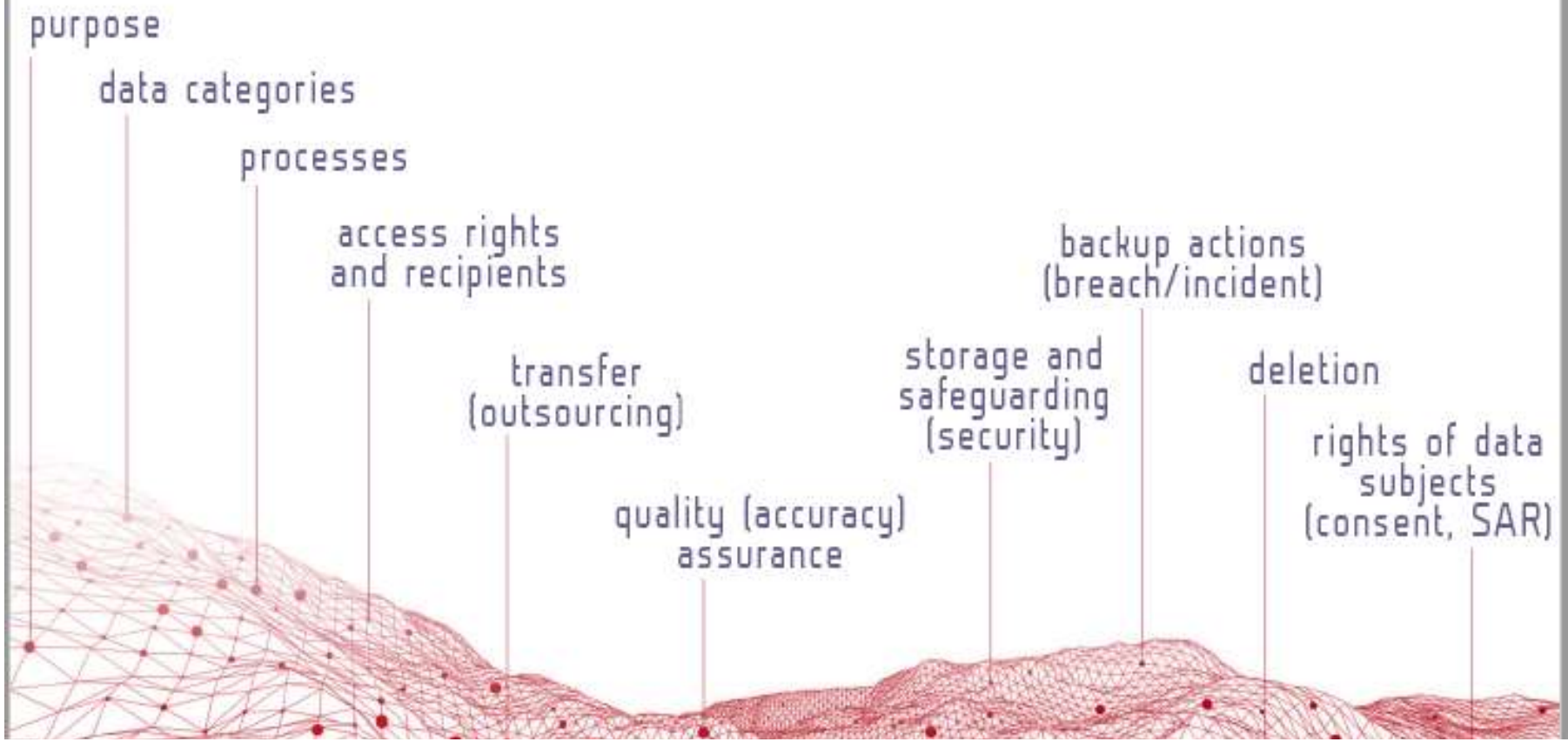
2.Identifying technical and organisational safety measures

After identifying the types of technology and organisational procedures that protect personal data…who has access to this information.

3.Understanding legal and regulatory requirements

Your final challenge is determining your organisation’s legal and regulatory obligations, retention schedules resulting.

dataMAPPING



BHConsulting

DATA MAPPING TEMPLATE # 1

Categories of personal data and data subjects	Elements of personal data included within each data category	Source of the personal data	Purposes for which personal data is processed	Legal basis for each processing purpose (non-special categories of personal data)	Special categories of personal data	Legal basis for processing special categories of personal data	Retention period	Action required to be GDPR compliant?
List the categories of data subjects and personal data collected and retained e.g. current employee data; retired employee data; customer data (sales information); marketing database; CCTV footage.	*List each type of personal data included within each category of personal data e.g. name, address, banking details, purchasing history, online browsing history, video and images.*	*List the source(s) of the personal data e.g. collected directly from individuals; from third parties (if third party identify the data controller as this information will be necessary to meet obligations under Article 14).*	*Within each category of personal data list the purposes for the data is collected and retained e.g. marketing, service enhancement, research, product development, systems integrity, HR matters, advertising.*	*For each purpose that personal data is processed, list the legal basis on which it is based e.g. consent, contract, legal obligation (Article 6).*	*If special categories of personal data are collected and retained, set out details of the nature of the data e.g. health, genetic, biometric data.*	*List the legal basis on which special categories of personal data are collected and retained e.g. explicit consent, legislative basis (Article 9).*	*For each category of personal data, list the period for which the data will be retained e.g. one month? one year?* *As a general rule data must be retained for no longer than is necessary for the purpose for which it was collected in the first place.*	*Identify actions that are required to ensure all personal data processing operations are GDPR compliant e.g. this may include deleting data where there is no further purpose for retention.*

BHConsulting

DATA MAPPING TEMPLATE # 2

Source	Personal Information	Data subject	Basis of processing	Data processing	Access	Disposal	Type of communication	Consent	Considerations					
									Consent obtained before May 25th	Consent needed	Subject is over 13/16	Critical data for the library	Sensitive personal data	ETC
How was this data collected?	What personal information are you collecting?	Who is the subject providing you the data?	Why are you collecting this data?	Explain how you will store this data and how it will be processed	Who has access to it and why?	When is this data disposed?	What type of comunication on have you received opt-in for?	How did you obtain consent?	Y/N	Y/N	Y/N	Y/N	Y/N	Y/N

BHConsulting

DATA MAPPING TEMPLATE # 3

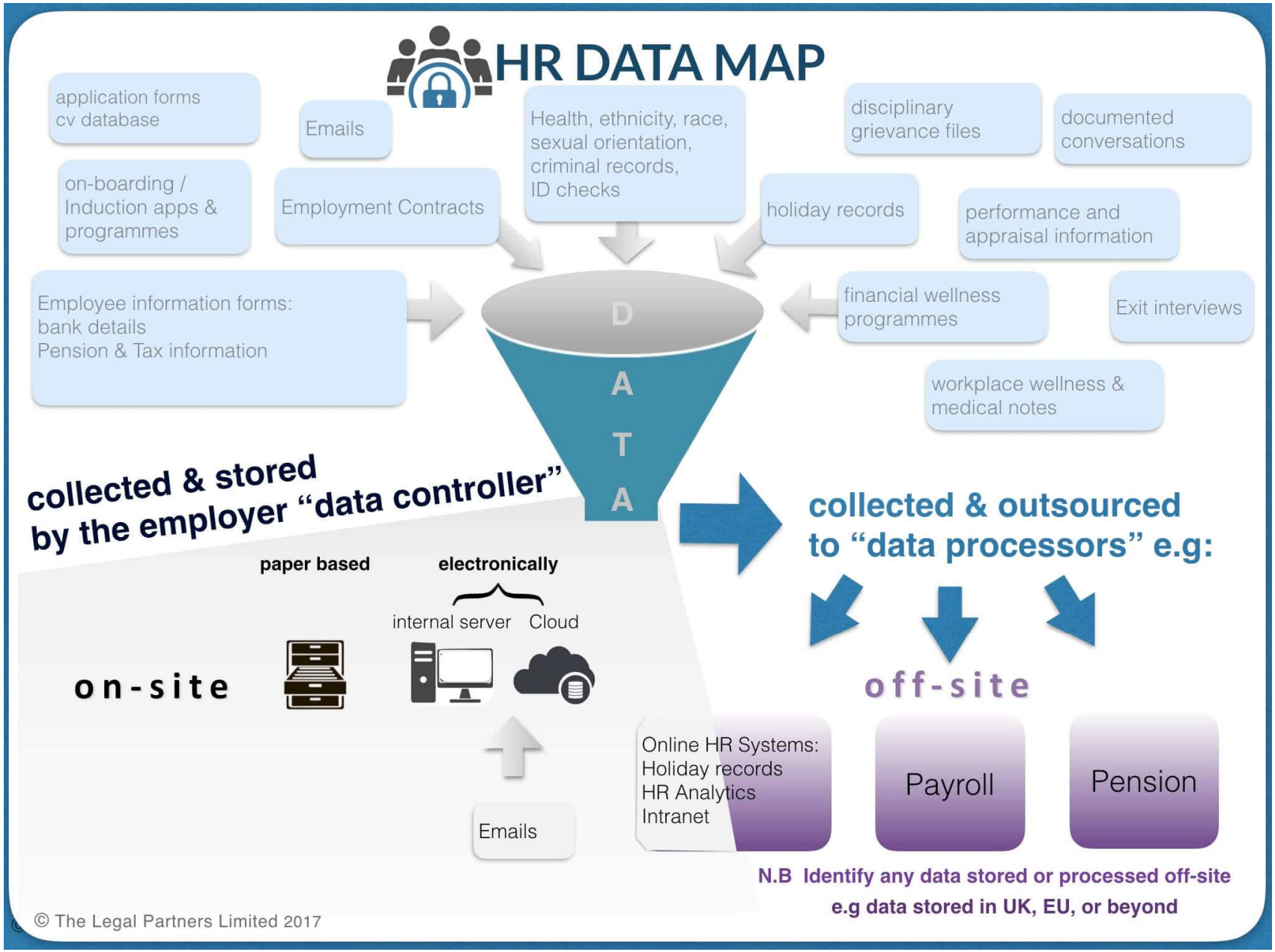
Overview										
Process Overview	**Volume of data**	**Type of data processed**	**Description of processing**	**New/Existing data?**	**Security**	**Who can access?**	**Information Owner**	**Observations**	**Actions**	**Compliant?**
Payroll - core	114 per month	Hardcopy data for new starters (P45/46 etc.), Hardcopy data for commissions. Electronic data for core tasks, emailed payslips.	Monthly processing of payroll information for staff including commissions, SSP, SMP, leaver and holiday pay. New starters/leavers processed as required.	Both (if new starters)	Core Sage payroll data files encrypted. Payslips password protected. Data directory restricted access. Finance only given sufficient data to do Management accounts.	Operations Director, MD only through core Sage application. MD, OD & head of tech ops for network file location.	Operations Director	Linking Sage payroll to NAV would reduce finance need to see data to do management accounts.	Investigate Payroll-NAV link	Compliant
Payroll - Pension										
Payroll - SAYE										
Payroll - Banking										

BHConsulting

DATA MAPPING TEMPLATE # 4

PURPOSE	WHOSE DATA	WHAT			WHEN		WHERE
		Type	Source	Legal basis	Updated	Retention Period	
Digital Marketing	Existing customers	Name Address Email Mobile Phone	Individual	Contract	As required	End of relationship	Marketing provider
	Potential customers	Name Email	Third party list	Consent of individual		Consent withdrawn	CRM locally stored
HR	Employee	Name Address Contact details Health details CV	Individual	Contract	As required As required Regularly As required No	Five years after termination	HR manual records in CRM

BHConsulting



DATA MAPPING DONE CORRECTLY : INFORMS SAR

- Where is data stored?
- Who is the data shared with?
- What is personal data? Sensitive Personal Data? Special Categories of data?
- What is the LEGAL BASIS FOR PROCESSING
- What secure measurements/safeguards or organisational processes do you have in place for protecting the information in line with risk to the DS?
- What is the retention schedule for the data
- What is the purpose/repurpose for the data
- What is the deletion/archival process for the data

BH Consulting

DATA MAPPING WORKSHOP EXERCISE #1

Complete a data map for (3) processes in your organisation/dept

- ***Choose a template, write key headings and fill in each box***
- ***Complete the template for at least three processes***

How many legal basis did you have?

How are you going to archive/delete?

Biggest Challenge?

BHConsulting

Systems to Consider

Booking Enquiries

Website, Website Cookies

Payments

Email Marketing

Social Media Marketing

Customer databases

Employee and HR Systems

Warning : Surveillance!!

DATA MAPPING WORKSHOP EXERCISE #2

Complete a data map for:

1. ***the recording of CCTV inside the building***
2. ***the recording of CCTV outside the building***

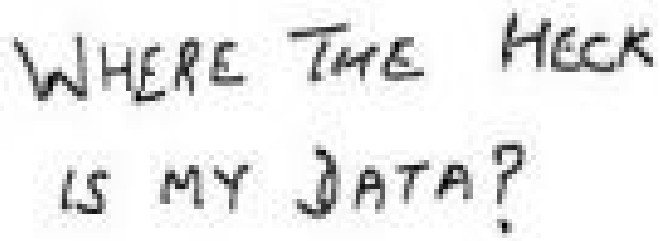
How many legal basis did you have?

How are you going to archive/delete?

Biggest Challenge?

Subject Access Requests

BHConsulting



Subject Access Requests

BH Consulting

GDPR DATA SUBJECT RIGHTS?

1. Right to be informed (Articles 13 & 14)
2. Right of access (Article 15)
3. Right to rectification (Article16)
4. Right to erasure (Article 17)
5. Right to restriction of processing (Article 18)
6. Right to data portability (Article 20)
7. Right to object (Article 21)
8. Automated individual decision making (Article 22)
9. Right to withdraw consent (Article 7)

BHConsulting

WHO IS A DATA SUBJECT?

- Natural Person (not a legal entity)
- Typically Customer, Client, Citizen or Employee
- (Third Parties, Solicitors, Contractors, Suppliers)

Why are they making a subject access request?

Data Access Requests under General Data Protection Regulation (GDPR)

Description of Action	General Data Protection Regulation (from May 25th 2018)
Fee	No Fee
Response time	One Month
Extensions to response time	Extension to a maximum of 3 months for complex requests: a. informing the data subject within one month of making the request and b. informing the data subject reason for the delay
Unfounded or excessive requests	**Controller has a choice of** a. charging a resonable fee to cover costs of responding to the request ***or*** b. Refusing to act on the request Burden of proof of excessive or unfounded request is with the data controller
Declining an access request	**Controller must inform the data subject of refusal to respond** a. within one month b. give reason for refusal
Form of response	**Controller must provide the information in concise, transparent, intelligible and easily accessible form** a. Clear and plain language b. Particular attention to information addressed specifically to a child
Format of response	**Controller must provide the information in writing, or by electronic means.** When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.
Identify of data subject	Where the controller has reasonable doubts concerning the identity of the natural person making the request referred, the controller may request the provision of additional information necessary to confirm the identity of the data subject

BHConsulting

PREPARING FOR A SAR?

1	Conduct a Data and System Inventory
2	Review and Update Privacy Policies and Notices
3	Draft and Implement an Internal Process or Checklist
4	Decide Architecture Framework
5	Train Your Employees
6	Enabling Data Subject Requests
7	Organize Data Subject Requests
8	Queue Management & Automation
9	Fulfillment of Request
10	Reporting & Metrics

BHConsulting

SUBJECT ACCESS REQUEST DISCLOSURE

In addition to a copy of their personal data, you must provide individuals with:

- The contact details of the DPO
- The purposes and legal basis for processing
- Where processing is based on legitimate interest, what the legitimate interests are
- The recipients or categories of recipients of the personal data
- Any cross-border data transfers (including the mechanism used if transfer is external to EEA and not covered by an adequacy decision)
- Retention period for personal data collected (or criteria used to determine the period)
- The existence of DS rights.
- Where processing is based on consent, the right to withdraw consent at any time
- The right to lodge a complaint with a DPA
- The existence of automated decision-making (including profiling) & meaningful information about the logic involved, the significance and the envisaged consequences

SARS CHECKLIST

PREPARING FOR A SAR:

☐ We know how to recognise a SAR and we understand when the right of access applies.
☐ We have a policy for how to record requests received verbally.
☐ We understand when to refuse a SAR and are aware of how to respond/include to DS.
☐ We understand the nature of the supplementary information we need to provide in response to a SAR.

COMPLYING WITH A SAR:

☐ We have processes in place to ensure that we respond to a SAR without delay, within 1 month of receipt.
☐ We are aware of the circumstances when we can extend the time limit to respond to a request.
☐ We understand that there is a particular emphasis on using clear and plain language if we are disclosing information to a child.
☐ We understand what we need to consider if a request includes information about others.
☐ We understand what to do if there are other data subjects mentioned in the information

Workshop SARs

Using the SAR Checklist, outline the three biggest challenges your group can determine from the SAR process. How might you address these?

Who will make the SARs?
Why will they submit a request for access to their information?
What about employees

Workshop SARs

You have received a request from a community centre user/renter, asking for a copy of all payments made by them and email correspondence for the last two years. You are aware that they are disputing the receipt/payments made.

Write a 5 step process.

BHConsulting

BHConsulting

Policies, Statements and Notices??

BH Consulting

DEFINITIONS AND BACKGROUND

A **Privacy Policy** is fundamentally a **document** for **internal** reference.

A **Privacy Statement** however is a document outlining how the organisation applies the **data protection** principles to data processed on its website.

A **Privacy Notice** is typically on a form or a website at the point of collection and provides transparency information to the data subject about the processing of the data

(Source DPC)

In 2010, Facebook's privacy policy was longer than the US Constitution. GDPR says information must be:
concise, transparent, intelligible and easily accessible; written in clear and plain language, particularly if addressed to a child; and free of charge. This means a simple link to your crazy-long privacy policy during registration will likely not do the trick.

Microsoft

Microsoft Privacy Statement

Expand All

Print

Last Updated: **June 2017** What's new?

Your privacy is important to us. This privacy statement explains what personal data we collect from you and how we use it. We encourage you to read the summaries below and to click on "Learn More" if you'd like more information on a particular topic.

The product-specific details sections provide additional information relevant to particular Microsoft products. This statement applies to the Microsoft products listed below, as well as other Microsoft products that display this statement. References to Microsoft products in this statement include Microsoft services, websites, apps, software and devices.

Personal Data We Collect

How We Use Personal Data

Reasons We Share Personal Data

How to Access & Control Your Personal Data

Cookies & Similar Technologies

Microsoft account

Other Important Privacy Information

Product-specific details:

Bing

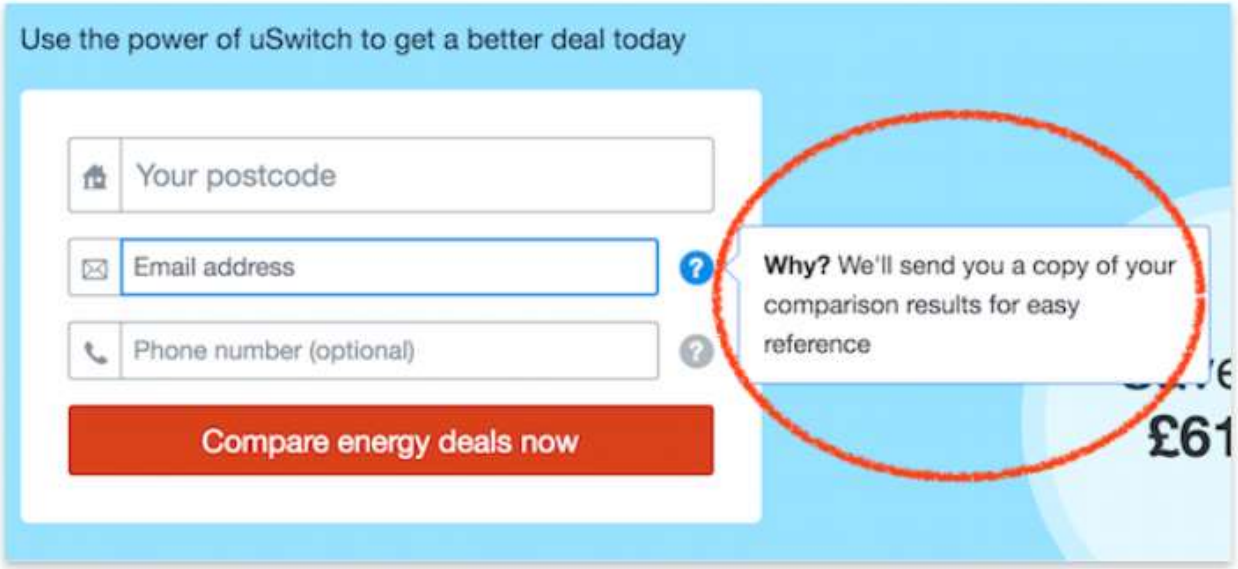
Personal Data We Collect

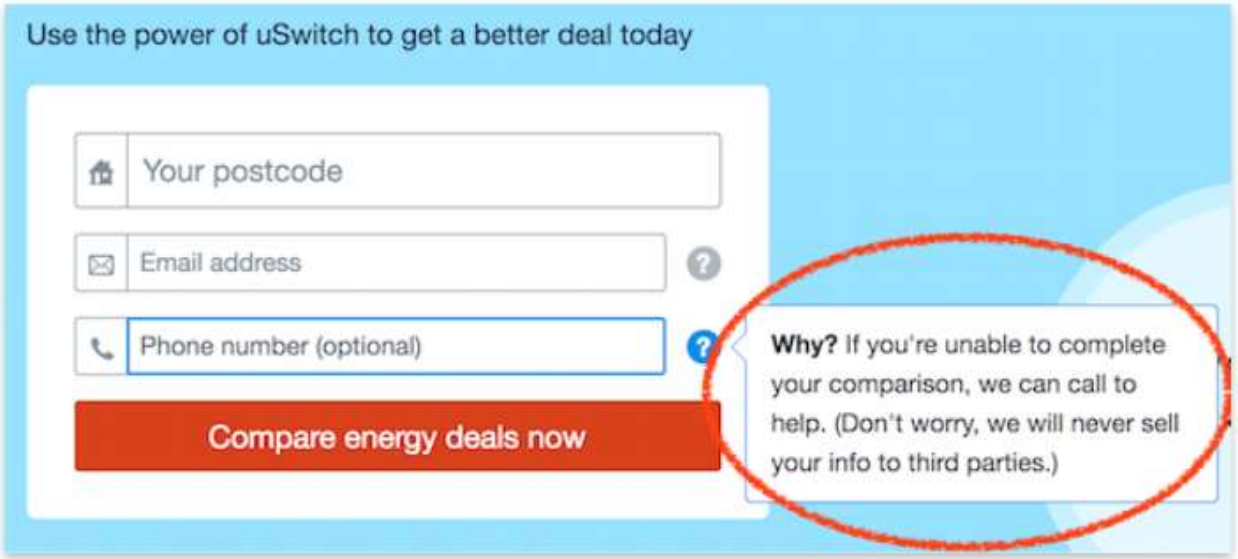
Microsoft collects data to operate effectively and provide you the best experiences with our products. You provide some of this data directly, such as when you create a Microsoft account, submit a search query to Bing, speak a voice command to Cortana, upload a document to OneDrive, purchase an MSDN subscription, sign up for Office 365, or contact us for support. We get some of it by recording how you interact with our products by, for example, using technologies like cookies, and receiving error reports or usage data from software running on your device. We also obtain data from third parties.

Learn More

Top of page

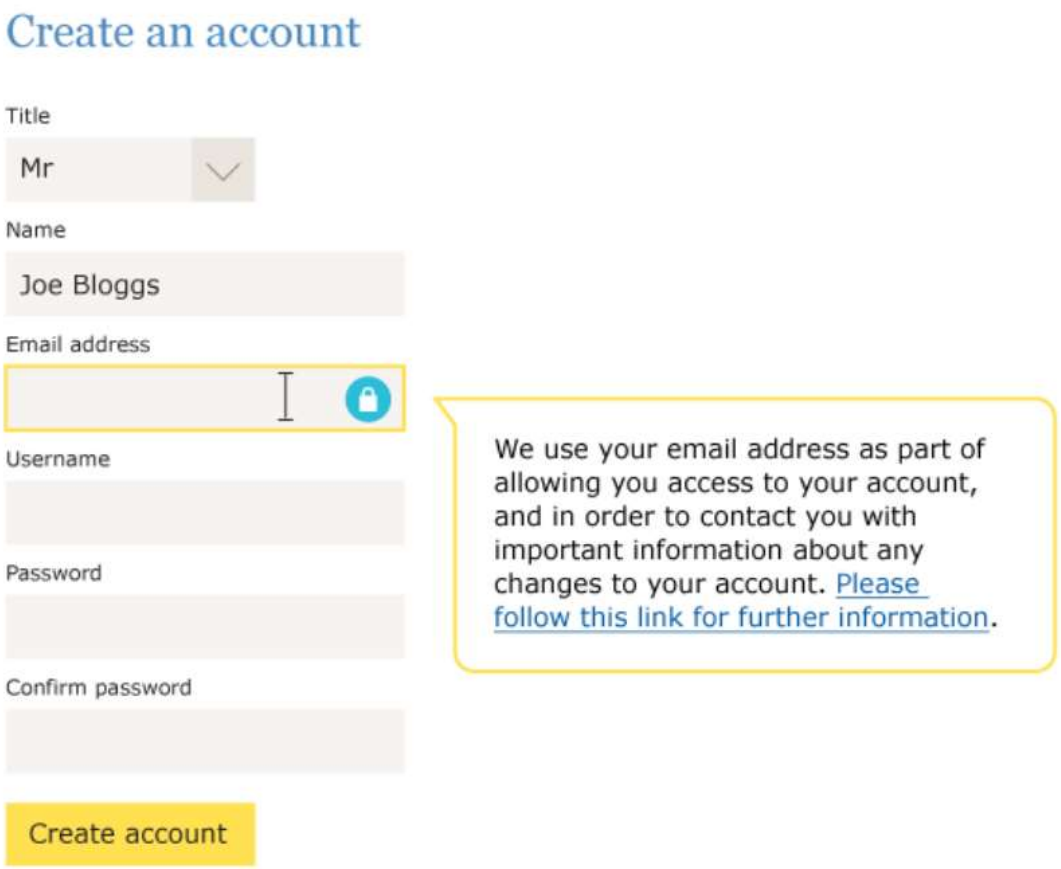
BHConsulting



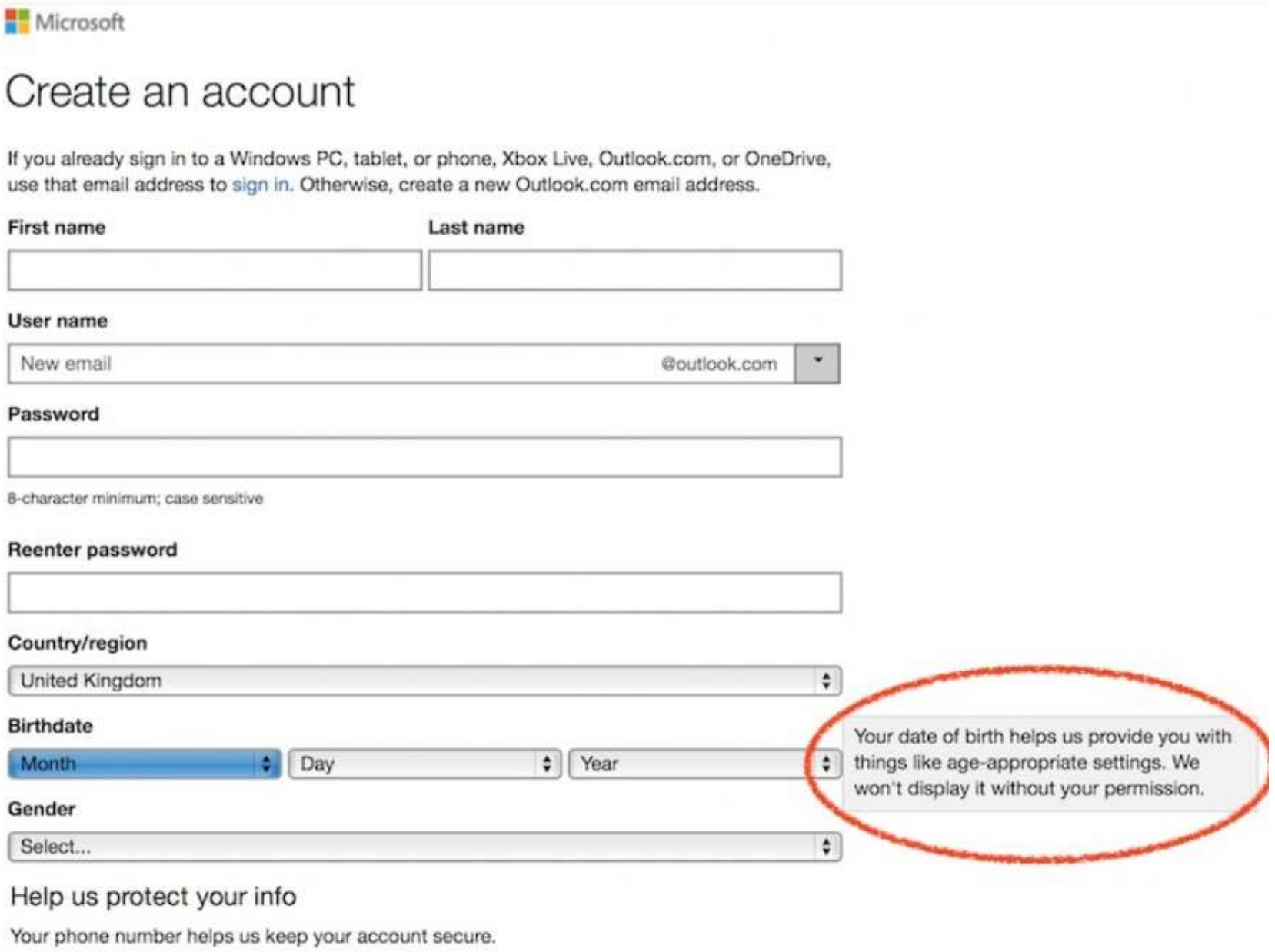


BHConsulting

PRIVACY NOTICE



BHConsulting



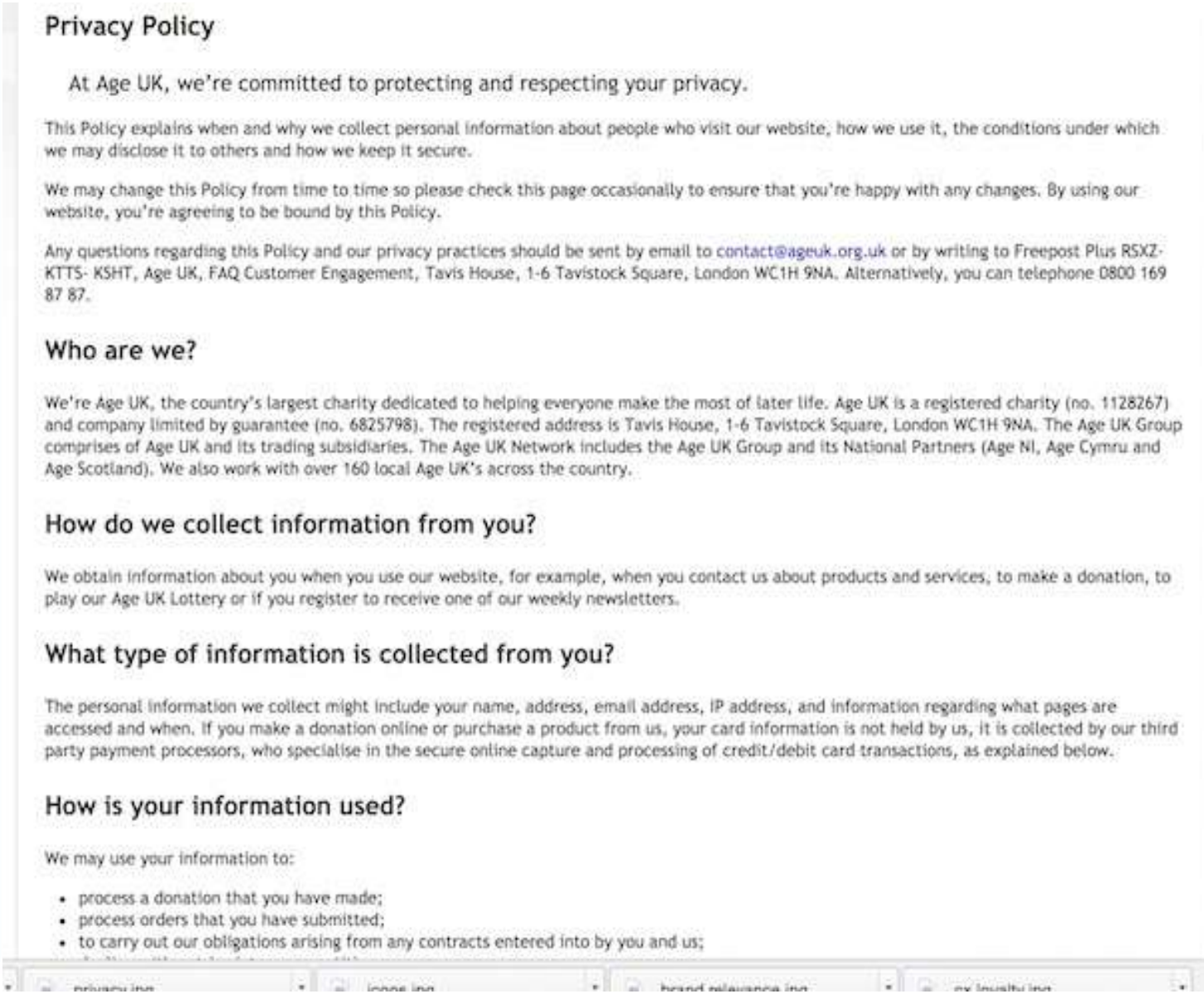
We'd like to keep in touch with you about the vital work we do for older people, our fundraising appeals and opportunities to support us, as well as the products and services you can buy.

We will never sell your data and we promise to keep your details safe and secure.

You can change your mind at any time by emailing contact@ageuk.org.uk

"We", includes the charity, its charitable and trading subsidiaries, and national charities (Age Cymru, Age Scotland and Age NI).

For further details on how your data is used and stored: www.ageuk.org.uk/help/privacy-policy



Privacy Policy

At Age UK, we're committed to protecting and respecting your privacy.

This Policy explains when and why we collect personal information about people who visit our website, how we use it, the conditions under which we may disclose it to others and how we keep it secure.

We may change this Policy from time to time so please check this page occasionally to ensure that you're happy with any changes. By using our website, you're agreeing to be bound by this Policy.

Any questions regarding this Policy and our privacy practices should be sent by email to contact@ageuk.org.uk or by writing to Freepost Plus RSXZ-KTTS- KSHT, Age UK, FAQ Customer Engagement, Tavis House, 1-6 Tavistock Square, London WC1H 9NA. Alternatively, you can telephone 0800 169 87 87.

Who are we?

We're Age UK, the country's largest charity dedicated to helping everyone make the most of later life. Age UK is a registered charity (no. 1128267) and company limited by guarantee (no. 6825798). The registered address is Tavis House, 1-6 Tavistock Square, London WC1H 9NA. The Age UK Group comprises of Age UK and its trading subsidiaries. The Age UK Network includes the Age UK Group and its National Partners (Age NI, Age Cymru and Age Scotland). We also work with over 160 local Age UK's across the country.

How do we collect information from you?

We obtain information about you when you use our website, for example, when you contact us about products and services, to make a donation, to play our Age UK Lottery or if you register to receive one of our weekly newsletters.

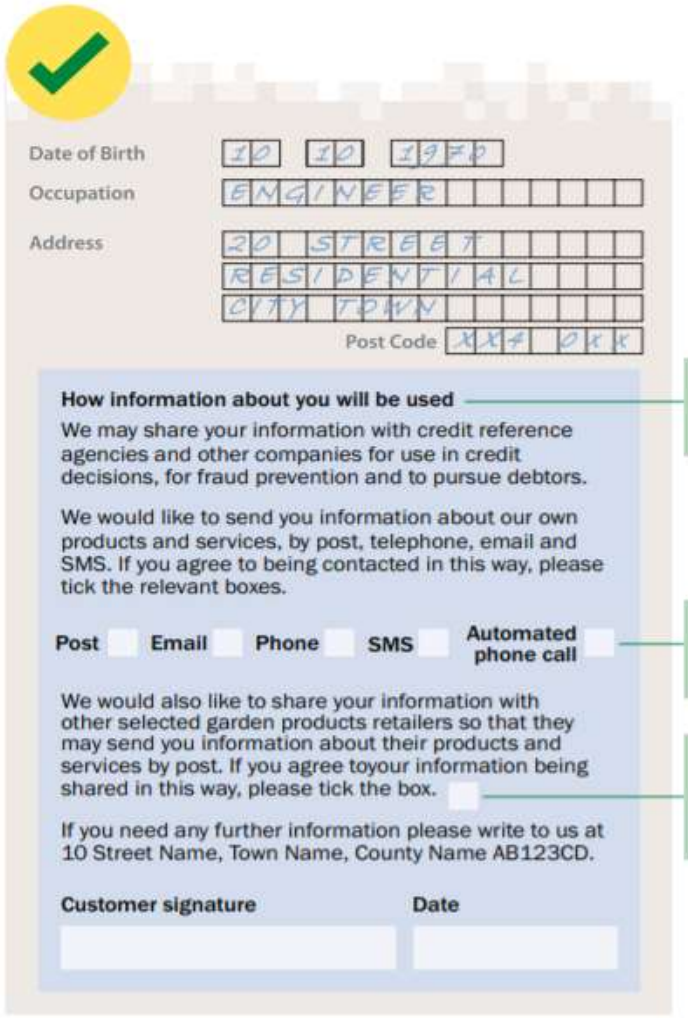
What type of information is collected from you?

The personal information we collect might include your name, address, email address, IP address, and information regarding what pages are accessed and when. If you make a donation online or purchase a product from us, your card information is not held by us, it is collected by our third party payment processors, who specialise in the secure online capture and processing of credit/debit card transactions, as explained below.

How is your information used?

We may use your information to:

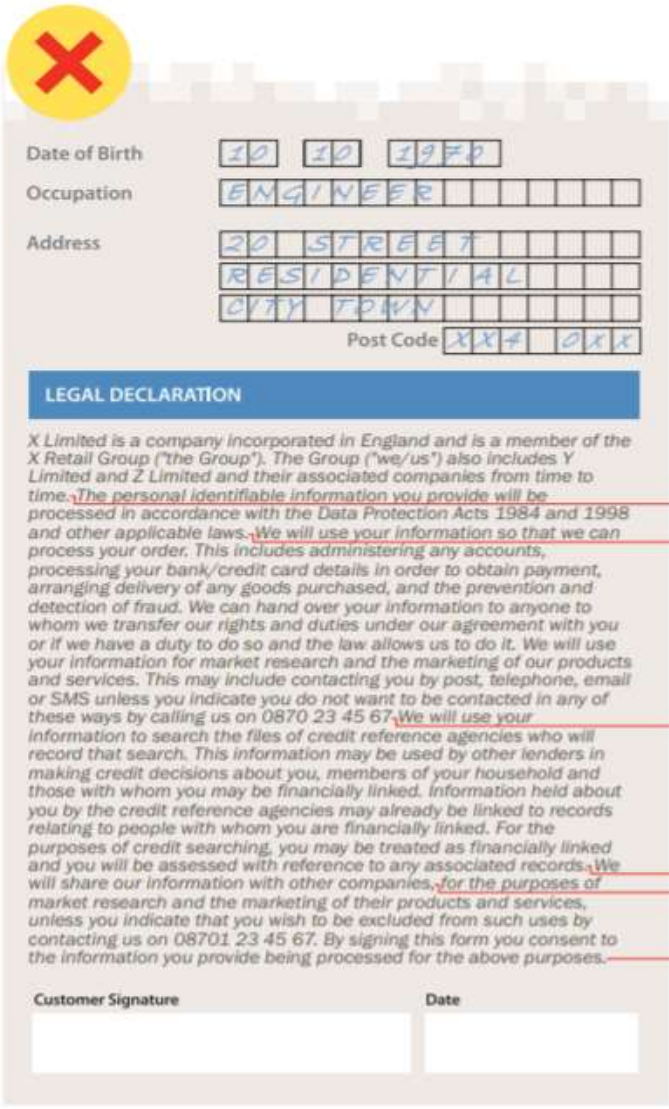
- process a donation that you have made;
- process orders that you have submitted;
- to carry out our obligations arising from any contracts entered into by you and us;



Simple language, clear font and style.

Clear opportunity to agree to marketing.

Prior consent sought for postal marketing by other companies.



Confusing and legalistic language. Closely spaced text, small italic font in light grey.

Unnecessary – means little to the public.

Specific opt-in consent is required for some e-marketing and is good practice for all direct marketing.

Confusing language.

No details of what type of companies.

Bad practice to seek one consent for several types of processing.

GROUP EXERCISE # 3

Document intended for internal guidelines	Privacy Notice
Document intended for DS notification on privacy terms	Privacy Statement
Disclosure of privacy terms at collection point	Privacy Policy

Design a ‘privacy notice’ for a key data collection process in your group.