protecture
DATA PROTECTION SUPPORT

Meeting all your data protection and privacy needs

Data Protection

CPRE

Suze Phillips Data Protection Lead

GDPR

*”…the **protection of natural persons** in relation to the processing of personal data is a fundamental right..."*

protecture
DATA PROTECTION SUPPORT

Protection….. Members, donors, volunteers

Trust…..wider community

Decision making….. sharing information

It's the law…..compliance

So what?

protecture
DATA PROTECTION SUPPORT

It's about managing risk...

* to individual rights and freedoms
* to the organisation
* to society if data use is uncontrolled

protecture
DATA PROTECTION SUPPORT

€20,000,000
or 4% of turnover

"…..as the Regulators, we actually prefer the carrot to the stick…..

….. it's a real opportunity for organisations to present themselves on the basis of how they respect the privacy and dignity of individuals."

protecture
DATA PROTECTION SUPPORT

Talking about an evolution

Council of Europe Convention 1981

➡ **Data Protection Act 1984**

An Act to regulate the use of automatically processed information relating to individuals and the provision of services in respect of such information

European Data Protection Directive 1995

➡ **Data Protection Act 1998**

An Act to make new provision for the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information

General Data Protection Regulation (Regulation (EU) 2016/679)

Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data

protecture
DATA PROTECTION SUPPORT

Principles

GDPR	Data Protection Act 1998
a) Lawfulness, fairness and transparency	1. Be processed fairly and lawfully
b) Purpose limitation	2. Obtained only for one or more lawful purposes……
c) Data minimisation	3. Be adequate, relevant and not excessive …..
d) Accuracy	4. Be accurate and, where necessary, kept up to date
e) Storage limitation	5. Not be kept for longer than is necessary…..
Rights	6. Be processed in accordance with …rights…
f) Integrity and confidentiality	7. Appropriate technical and organisational measures
Transfers	8. Shall not be transferred to a country or territory outside the EEA…

protecture
DATA PROTECTION SUPPORT

Personal Data

* Information relating to an **identified** or **identifiable** natural person…. who can be identified, directly or indirectly,….. by reference to an identifier such as a name, an identification number, location data, an online identifier or….the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

protecture
DATA PROTECTION SUPPORT

Is it personal data?

* **John Smith** on a Post-It note in the street
* **John Smith** on a Post-It note on a desk
* A physical description of you in an email

Who are your data subjects?

* Members
* Campaign supporters
* Subscribers
* Volunteers
* Trustees
* Staff

protecture
DATA PROTECTION SUPPORT

What do we mean by Processing ?

* Any operation or set of operations
* collecting, recording, organising, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
* Whether or not automated

protecture
DATA PROTECTION SUPPORT

Data Controller

"….the natural or legal person, public authority, agency or other body which, alone or jointly with others, ***determines the purposes and means*** *of the processing of personal data…."*

protecture
DATA PROTECTION SUPPORT

Data Processor

"….a natural or legal person, public authority, agency or other body which processes personal data ***on behalf of*** *the controller"*

protecture
DATA PROTECTION SUPPORT

the controller **and the processor** shall implement appropriate technical and organisational measures…

Data Controller → **Data Processor**

Contract

CPRE

Mailing house

Secretarial service

Event management

Payroll

Principles

GDPR

a) Lawfulness, fairness and transparency

b) Purpose limitation

c) Data minimisation

d) Accuracy

e) Storage limitation

f) Integrity and confidentiality

"The Controller shall be responsible for, and **be able to demonstrate compliance** with….."

must comply with all, for the processing to be lawful

protecture
DATA PROTECTION SUPPORT

Lawfulness, fairness & transparency

* Is your use of the personal data justified?
* What would people reasonably expect?
* Is it fair?

protecture
DATA PROTECTION SUPPORT

Purpose limitation

* Is it okay to use it for some other purpose?
* Is it something new or similar to before?

Data minimisation

* Do I even need to use personal data?
* How much detail do I **need**?

protecture
DATA PROTECTION SUPPORT

Accuracy

* How am I going to record this accurately?
* How accurate does it **need** to be?
* Does it **need** to be kept up to date?

protecture
DATA PROTECTION SUPPORT

Storage Limitation

* How long should I keep this personal data for?
* Does it **need** to be kept as personal data?
* How should I dispose of it?

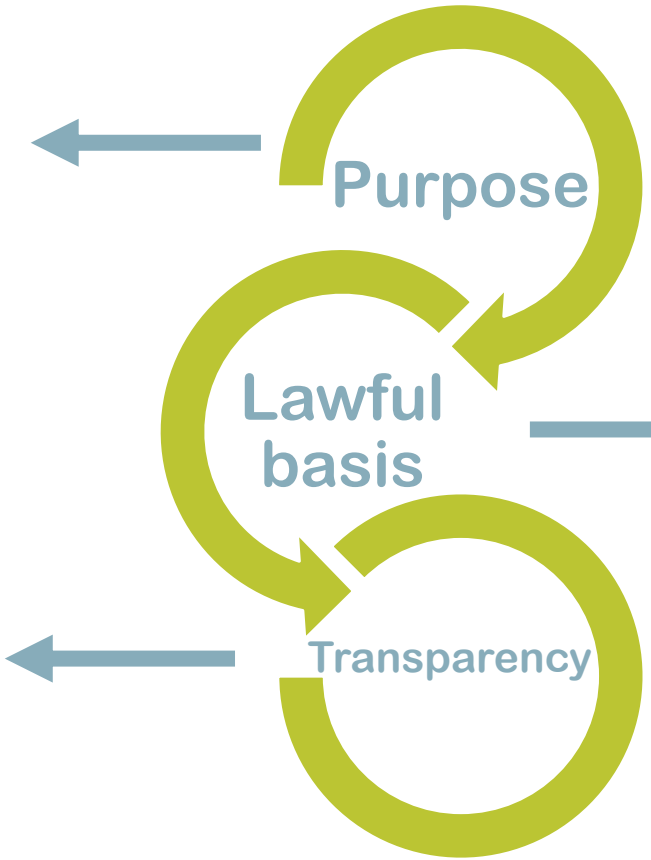
protecture
DATA PROTECTION SUPPORT

Security

* How do I keep personal data secure?
* What about confidentiality?

protecture
DATA PROTECTION SUPPORT

* What it's used for
* Who it's shared with
* How long it's kept



Link to extent to which people can enforce their rights

Privacy Information

Purpose

(what are you using the personal data to do?)

Lawful Basis

- Taking donations
- Paying staff
- Publishing case studies
- Recruiting volunteers
- Convening meetings
- Holding events

"…communication (by whatever means) …of any advertising or marketing material …which is directed to particular individuals".

"All promotional material….including material promoting the aims [and ideals] of not-for-profit organisations…

…any messages which include some marketing elements, even if that is not their main purpose.

PECR (2003)

The Privacy and Electronic Communications (EC Directive) Regulations 2003 sets out specific privacy rights on electronic communications.

PECR covers:

- Marketing by electronic means, including **marketing calls, texts, emails and faxes**.
- The use of cookies that track information about people accessing a website or other electronic service.
- Security of public electronic communications services.
- Privacy of customers using communications networks or services as regards traffic and location data, itemised billing, line identification services (eg caller ID and call return), and directory listings.

protecture
DATA PROTECTION SUPPORT

Lawful Basis

Consent of the data subject

For the performance of a **contract** with the data subject or to take steps to enter into a contract

For compliance with a **legal obligation**

Necessary to protect the **vital interests** of a data subject or another person

Necessary for the performance of a **task carried out in the public interest** or in the exercise of official authority vested in the controller

Necessary for the purposes of **legitimate interests** pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

protecture
DATA PROTECTION SUPPORT

Consent

Any **freely given**, **specific**, **informed** and **unambiguous indication** of [their] wishes…[either] by a **statement** or by a **clear affirmative action**

protecture
DATA PROTECTION SUPPORT

Consent

* Shall be **able to demonstrate** that [they] **consented**
* The **right to withdraw** consent at any time…it shall be as easy to withdraw as to give consent
* **Not** freely given if they had "**no genuine or free choice** or is **unable to refuse or withdraw consent without detriment**"
* **Effective audit trail** of how and when consent was given

Clear affirmative action

1. Signing a consent statement on a form
2. Ticking a box on a form or on screen (not pre-ticked)
3. Clicking on a button or link
4. Selecting from yes/no options – that were presented equally
5. Sending an email confirming consent
6. Filling in options on a preference dashboard
7. Saying yes to a clear verbal question seeking consent

protecture
DATA PROTECTION SUPPORT

Legitimate Interests

- Clear business objective
- How necessary is the personal data
- Relationship and expectations
- Identify potential harm
- Needs careful consideration – balancing of interests
- Publication of balancing exercise
- Can include direct marketing

Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject

protecture
DATA PROTECTION SUPPORT

Lawful Basis

Consent (direct marketing by email or sms, case studies)

Contract (membership, sales)

Legal Obligation (H&S, gift aid)

Vital Interests (life and death situations)

Task carried out in the public interest (education, healthcare)

Legitimate interests (direct marketing by post, providing information, taking donations)

protecture
DATA PROTECTION SUPPORT

Purpose	Lawful Basis
Taking donations	Legitimate interest
Paying staff	Contract
Publishing case studies	Consent
Recruiting volunteers	Legitimate interest
Membership	Contract
Holding events	Legitimate interest

Transparency

Can you explain what you're doing with personal data if you're asked?

Do you know how to find or signpost to the CPRE privacy information?

protecture
DATA PROTECTION SUPPORT

Rights

Right to be Informed

Right of Access

Right to Rectification

- Make sure you can identify a request
- Know what personal data you've got and where it is
- Know the lawful basis for your use of the personal data
- Have a process in place to respond within the 30 days time limit

Right to Erasure (Right to be forgotten)

Right to Restrict Processing

Right to Data Portability

Right to Object

Rights in relation to Automated Decision Making

protecture
DATA PROTECTION SUPPORT

Right	Lawful Basis					
	Consent	Contract	Legal Obligation	Vital Interests	Public Task	Legitimate Interests
Access				✓		
Rectification				✓		
Restriction				✓		
Erasure	✓	✓				✓
Object					✓	✓
Portability	✓	✓				
In relation to automated decision making					✓	✓

protecture
DATA PROTECTION SUPPORT

Special Category Data

racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, **genetic data, biometric data,** data concerning health or data concerning a natural person's sex life or sexual orientation

- Employment (reasonable adjustments, equalities monitoring, occupational health…)
- Events (accessibility, dietary requirements…)

protecture
DATA PROTECTION SUPPORT

Data Protection Officer

- ✓ Public Authority
- ✓ Core activities……. require regular and systematic monitoring….on a large scale
- ✓ Core activities….large scale of special categories of data…criminal convictions…

- **Inform and advise**
- **Monitor compliance**
- **DP Impact Assessment**
- **Co-operate with ICO**

"He or she shall not be dismissed or penalised…for performing his tasks….. the data protection officer shall report directly to the highest management level…".

protecture
DATA PROTECTION SUPPORT

Security

protecture
DATA PROTECTION SUPPORT

Security

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk…….

protecture
DATA PROTECTION SUPPORT

Security

Lost Mobile devices

Physical access to paper records

Phishing or Spear Phishing

Unpatched software

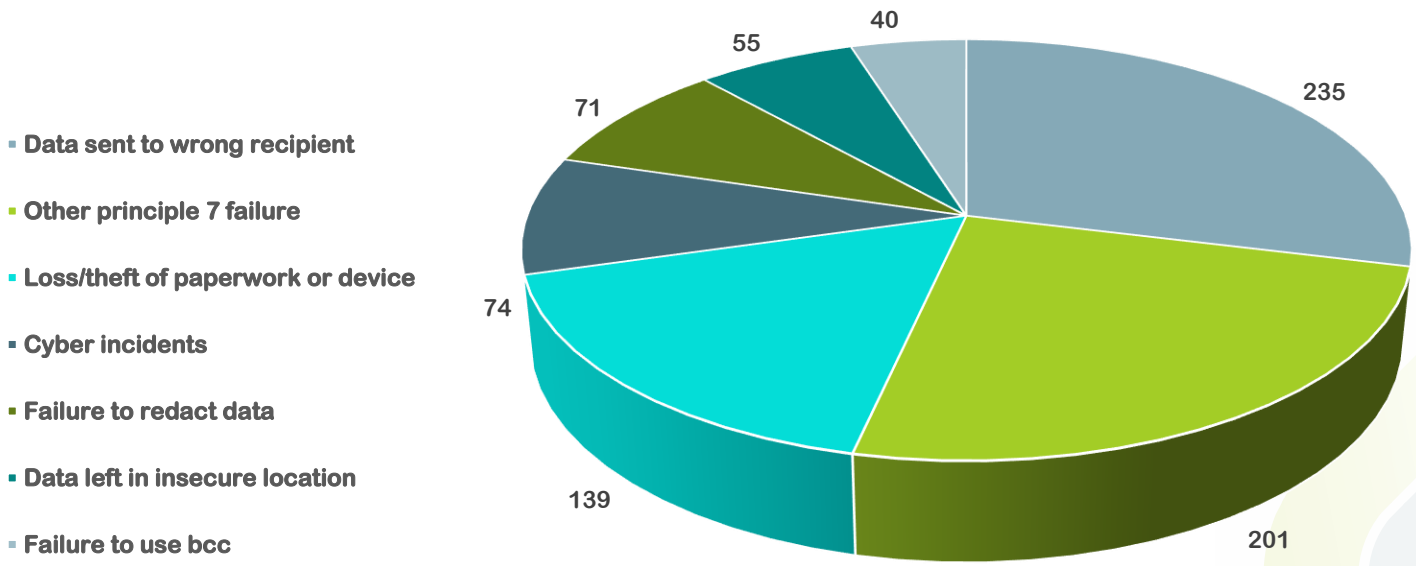
Poorly configured IT

Human error **Malicious acts**

- Destruction: where the data no longer exists, or no longer exists in a form that is of use
- Damage: where data has been altered, corrupted, or is no longer complete
- Loss: data may still exist, but the controller has lost control or access to it, or no longer has it in its possession
- Unauthorised or unlawful processing: may include disclosure of personal data to (or access by) recipients who are not authorised to receive or access the data

protecture
DATA PROTECTION SUPPORT

There were 815 data incidents reported to the ICO in Q3, 41% increase on Q3 2016



protecture
DATA PROTECTION SUPPORT

Security

- Staff and Volunteer Training
- Keep track of where your data is
- Install Patches and security updates
- Use Encryption
- Use Passwords
- Secure storage and disposal
- Formal leavers process
- 3rd parties and procurement

protecture
DATA PROTECTION SUPPORT

Data Breach

1. Gather information on the incident
2. Take immediate action
3. Assess the risks
4. Notify & liaise with the authorities
5. Communicate with individuals
6. Document the Incident
7. Review the outcomes

protecture
DATA PROTECTION SUPPORT

Breach Notification

If the breach is **likely to result in a risk** to the rights and freedoms of individuals, then the Information Commissioner must be notified

If the breach is **likely to result in a high risk** to their rights and freedoms, this needs to be communicated to the individuals **without undue delay**

72 Hours

Physical harm

Identity theft

Fraud

Financial loss

Discrimination

protecture
DATA PROTECTION SUPPORT

Q & A

020 3691 5731
www.protecture.org.uk
help@protecture.org.uk
@ProtectureDPO