



The GDPR

David Green
Green Pepper

Contents...

- What is it?
- In what circumstances does it apply?
- What does it do?
- What does it mean for us?

What is it

- A new regulation from Europe
- Providing extended rights to individuals
- Requiring much greater transparency
- With very large fines for serious breaches
- Effective 25 May



**FUNDRAISING
REGULATOR**



**CHARITY COMMISSION
FOR ENGLAND AND WALES**

When does it apply...

- Processing any info from which a *person* could be identified
- Whether automated or manual systems
- Covers controllers and processors of *personal* data

What does it do...

- Six data principles
- Must have lawful basis for processing data
- Special categories
- Rights of individuals
- Transparency
- Governance and accountability

Six data principles...

1. Processed lawfully, fairly and transparently
2. Collected for specified, explicit and legitimate purpose
3. Adequate, relevant and limited to what is necessary
4. Accurate and kept up-to-date
5. Kept for no longer than necessary
6. Processed in a secure manner

The lawful basis for data processing



1. Consent
2. Contractual
3. Legal obligation
4. Vital interest
5. Necessary to perform public task
6. Legitimate interest

Consent

- Freely given and unambiguous
- Affirmative (no pre-ticked boxes)
- Separate, not bundled or generic
- Evidenced
- Reviewed, and refreshed if anything changes

So would this be lawful...

By registering your details you indicate your consent for us to email you information about selected products, events and services from Charity X and from carefully chosen third parties unless you object to receiving such messages by ticking the boxes below.

I do not want to receive other emails from:

- I do not want to receive other emails from Charity X
- I do not want to receive emails from Third Parties

Consent transparency

When consent is given

- Identify your organisation
- Why you want the data
- What you will do with it
- Name of any third party processor
- That consent can be withdrawn

Contractual

- To fulfil contractual obligations, or
- Asked to take pre-contract action

Legal obligation

- To comply with the law
- Includes common law and statute

Vital interest

- To protect a person's life
- Applies if not even the data subject
- Does not apply if individual is capable of giving consent

Public interest

Necessary to perform:

- a task in public interest
- official functions

Legitimate interest

Appropriate if use data

- in a way people would reasonably expect
- and has minimal privacy impact
- or where a compelling justification

You must

- Identify your legitimate interest
- balance your interests against those of data subject

Assessing legitimate interest...

- Is it reasonable?
- Is this the only way?
- Would it be expected?
- Am I happy to explain it to the data subject?
- There will be no intrusive/harmful impact
- It does not override the interests of individual
- I can offer an opt-out

Legitimate interest examples..

- Using client or employee data
- Marketing
- Fraud prevention
- IT security

Special categories

- Same as current sensitive data, plus
- Biometric data
- But excludes criminal data (separate category)
- Also need a “condition” as well as lawful basis to process
- Additional considerations for children’s data

Rights of individuals

- To be informed
- To have access
- To have errors rectified
- To be forgotten
- To restrict
- To portability
- To object
- Relating to automated processing and profiling

Transparency...



Privacy notices/policies

- Identify organisation and named contact
- The lawful basis and purpose of processing
- The categories of data processed
- Details of third parties
- How long data is kept
- Data subject's rights
- If the data is required by law

Provision of information

- Clear and plain language
- Avoid words like “may” “might” “possibly” etc.
- When data is collected
- Not hidden away
- Layered where appropriate
- If further processing needed
- If lawful basis changes

Accountability

- Keep detailed records of processing operations
- Perform, data protection impact assessments (DPIA)
- Designate a Data Protection Officer
- Notify and record data breaches
- Be able to demonstrate compliance

What does this
mean for us?



To comply...

- A lawful basis for processing
- Meet the transparency requirements
- Uphold the rights of data subjects
- Meet any specific governance requirements

Compliance checking

1. Conduct a data audit
2. Decide which of the six lawful bases apply
3. Update as needed
 - data capture processes
 - privacy notices
 - other policies and procedures
 - governance measures
 - third party contracts

Data audit...

- What data do we collect?
- How do we collect it?
- Where is it processed?
- When or how often is it processed?
- What do we use it for?
- Who do we share it with?
- Where and how is it stored
- Is it needed, or could it be anonymised?

What is the lawful basis...

A reminder of the six:

1. Consent
2. Contractual
3. Legal obligation
4. Vital interest
5. Public interest
6. Legitimate interest

Update as needed

- Transparent privacy notices
- Wording on paper/website forms
- Do we need to seek consent again?
- Procedures allowing data subjects to enforce rights
- Procedures regarding data breaches
- Is DPO or DPIA necessary?
- GDPR compliant contracts with third parties
- Security measures

Direct marketing...

To individuals

- Email, text, automated call: consent needed (PECR 2003)
- Post or phone: consent or legitimate interest

To corporate subscribers

- Legitimate interest or consent for all methods



Further information

GDPR Workshop, 27 March at CVS Beds. Tickets £32

Details and other resources at <https://greenpepperconsulting.co.uk>

- ICO
- Fundraising Regulator
- NCVO
- Institute of Fundraising
- Data Protection Network

David Green

Twitter: @GreenPepper2016

green pepper 