Digital Interruption

Oh GEEE(DPR)

not testing too?

Functional mapping is literally my answer to everything

www.digitalinterruption.com

contact@digitalinterruption.com

our GDPR journey

- Overview of the regulation
- Governing principles
- How to be compliant
- Continuous integration
- Security tooling (sign post)

DIGITAL INTERRUPTION

whoami?

Saskia Coplans

@saskiacoplans

Co-founder of

@DI_Security & @mcrgreyhats

what is GDPR?

The **General Data Protection Regulation** (**GDPR**) is a regulation intend to **strengthen and unify data protection** for all individuals within the European Union (EU)

DIGITAL INTERRUPTION

the regulation

6 principles

99 articles

173 recitals

(it’s a riveting read)

DIGITAL INTERRUPTION

Article 5

Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(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 are 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(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 ('integrity and confidentiality').

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

what does this mean?

You must follow the **6 principles** of the regulation and you must **demonstrate compliance** against these principles

DIGITAL INTERRUPTION

principle 1

Lawful, fair & transparent

If you can't (or won't) ***explain*** *what you* ***do*** *with personal data, then you probably* ***shouldn't*** *be doing it*

principle 2

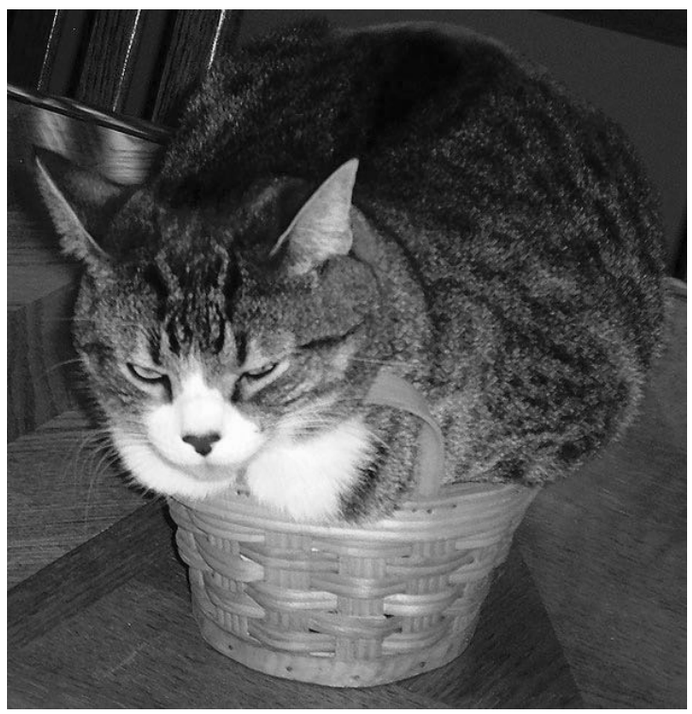
Purpose specific

*If you can't demonstrate **why** you need the data, then you **don't** need the data*

principle 3

Minimal (data minimisation)

Irrelevant *personal data poses an unnecessary security* ***risk*** *and can be* ***expensive*** *to store and secure*



principle 4

Accurate and up-to-date

*If it's not **accurate** or you no longer **need** it, either **correct** it or **delete** it*

principle 5

Time limited

Once it's expired ***delete*** *it, if you think you still need it* ***anonymise*** *it*

principle 6

Confidential and secure

*If it's **not** secure, it's **not** compliant*

*The best way to ensure that the data is secure? **Test it!***

being compliant

What does compliant look like?

DIGITAL INTERRUPTION

staying compliant

"implement **technical** and organisational measures to show that you have considered and **integrated** data protection into your processing activities"

DIGITAL INTERRUPTION

baked in

Bake security and compliance in to the **development pipeline**, and therefore reduce the **risk** of slipping back in to non compliancy

DIGITAL INTERRUPTION

what is personal data?

- user ID
- log details
- IP address
- ref numbers
- full name
- address
- email address
- date of birth
- phone number
- bank details
- cc numbers
- ugc
- images/photos
- emails
- recordings / transcripts
- location info
- cookies

DIGITAL INTERRUPTION

key purpose

What is it supposed to do?

To sell and distribute goods and services to customers worldwide through the use of a web application

DIGITAL INTERRUPTION

core functions

1. **Interface** - brows products/ reviews/contact us/T&C/FAQs/ email marketing
2. **Backend and storage** - data base to store products/ services/customer information/reviews
3. **Select** - put purchases in e-basket
4. **Pay** - enter payment details
5. **Shipping** - add delivery requirements
6. **Complete** - either follow up with queries or complaints

DIGITAL INTERRUPTION

requirement

- A user cannot log into the application without knowledge of the password
- Sensitive data should only be stored securely
- Personal data should be able to be corrected, deleted, restricted and exported
- Sensitive data should not be logged (in the back end)
- The application should behave correctly when malicious SQL characters are used in the application fields / sent to the application
- The application should behave correctly when a path containing directory navigation characters are sent to the application
- Sensitive data should not be transferred or tramped in plain text

DIGITAL INTERRUPTION

security tooling

Burp Suite or
Zap Proxy (Web apps)
Drozer (Android)
SQL Map (SQL injection)

recap

- Overview of the regulation
- Governing principles
- How to be compliant
- Continuous integration
- Security tooling (sign post)

DIGITAL INTERRUPTION

Digital Interruption

Oh GEEE(DPR)

not testing too?

Functional mapping is literally my answer to everything

saskia@digitalinterruption

@saskiacoplans/@jayHarris_Sec

@DI_Security

DIGITAL INTERRUPTION