General Data Protection Regulation (GDPR) – But without the hype

John Elliott  LLM CIPP/E  CISSP CISA CRISC FBCS
Regulation, privacy, security, risk & payments geek

@withoutfire
Disclaimers

• I am not a lawyer.
• The views expressed are mine alone and don’t represent those of my current employers or clients.
• This is EU law and so is written in British English.
Fear  Uncertainty  Doubt
Relief Uncertainty Knowledge
Agenda

Big Picture
Who, what, when, where, why, how

Detail
What’s does it actually say?

Prepare
What should you do?

Q&A
What would you like to know?
As a regulation geek

• Who does the regulation come from?
• What is the regulation trying to achieve?
• What does compliance look like?
• Do I want to comply (is it sensible/useful)?
• Do I have to comply (is it mandatory)?
• What happens if I don’t?
• What are the negative effects of compliance?
• What will I do – is there an MVP (MVC)?
Regulatory zones of compliance

- Playing Safe
- Probably OK
- "Perfect" compliance

degree of compliance

cost
Regulatory zones of compliance

- Money no object
- Playing Safe
- Probably OK
- Hope we’re lucky

“Perfect” compliance
Regulatory zones of compliance

- Money no object
- Playing Safe
- Probably OK
- Hope we’re lucky

regulatory risk appetite
Big Picture Context
European Union Law
Regulation for the protection of personal data.

4.5.2016  EN  Official Journal of the European Union  L 119/1

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 27 April 2016
on the protection of natural persons with regard to the processing of personal data and on the free
movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

(Text with EEA relevance)

Regulation for the protection of personal data.

‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’);
Regulation for the protection of personal data.

Natural person = living human being
Data Subject = someone whose data you have
25th May 2018
Last EU data protection law was in 1995 - the world has moved on and, because the last EU data protection thing was a Directive, it was applied randomly across the 28 EU contrived.

- Strengthen the rights of the individual over their own data (privacy)
- Make organisations accountable
No barrier to services acquired anywhere in the Union.

Ensure equal protection of EU human rights.
It’s an EU regulation.

That means it is the law in every EU Member State (and practically also the EU’s best friends)
Data Controller = organisation that has relationships with Data Subjects and “processes” their personal data

Data Processor = 3rd party that works for a Data Controller and processes personal data on its behalf
3(1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
3(2) This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

a) the offering of goods or services (irrespective of whether a payment of the data subject is required) to such data subjects in the Union; or

b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
RECITALS

Why we’re doing this and what we hope to achieve

(173)

Business Requirements

ARTICLES

The rules

(99)

Code
GDPR’s 99 Articles

- General and principles: 42%
- Data subject rights: 12%
- Controller Responsibilities: 11%
- Sending data out of the EU: 8%
- Remedies: 7%
- Administration: 3%

Who
What
When
Why
How
Who
Who
What

Security
Detail
Core Data Protection Principles

11 articles that define the core principles in the Regulation along with some useful definitions.
Core principles

Lawful, fair and transparent

Article 5(1)(a)
Core principles

Lawful, fair and transparent
Article 5(1)(a)

Expected by the person whose data it is
Article 5(1)(b)
Core principles

- **Lawful, fair and transparent** (Article 5(1)(a))
- **Expected by the person whose data it is** (Article 5(1)(b))
- **Just enough data to do what you’re doing** (Article 5(1)(c))
Core principles

- Lawful, fair and transparent
  Article 5(1)(a)

- Expected by the person whose data it is
  Article 5(1)(b)

- Just enough data to do what you’re doing
  Article 5(1)(c)

- Accurate
  Article 5(1)(d)
Core principles

Lawful, fair and transparent
Article 5(1)(a)

Expected by the person whose data it is
Article 5(1)(b)

Just enough data to do what you’re doing
Article 5(1)(c)

Accurate
Article 5(1)(d)

Only kept as long as necessary.
Article 5(1)(e)
Core principles

Lawful, fair and transparent
Article 5(1)(a)

Expected by the person whose data it is
Article 5(1)(b)

Just enough data to do what you’re doing
Article 5(1)(c)

Accurate
Article 5(1)(d)

Only kept as long as necessary.
Article 5(1)(e)

“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’)”

Article 5(1)(f)
Core principles

- **Lawful, fair and transparent**
  - Article 5(1)(a)

- **Expected by the person whose data it is**
  - Article 5(1)(b)

- **Just enough data to do what you’re doing**
  - Article 5(1)(c)

- **Accurate**
  - Article 5(1)(d)

- **Only kept as long as necessary.**
  - Article 5(1)(e)

“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’)”

Article 5(1)(f)

“The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’)”

Article 5(2)
Data Subject Rights

12 articles that describe the rights of Data Subjects in respect of the data that an organisation processes.
Under GDPR, Data Subjects have the right to ...

... know what’s going to be done with your data.
(Article 13)
Under GDPR, Data Subjects have the right to ...

... know what’s going to be done with your data. (Article 13)

... copies of all the data being processed. (Article 15)
Under GDPR, Data Subjects have the right to ...

... know what’s going to be done with your data.  
(Article 13)

... copies of all the data being processed.  
(Article 15)

... have incorrect data corrected.  
(Article 16)
Under GDPR, Data Subjects have the right to ...

- ... know what’s going to be done with your data. (Article 13)
- ... copies of all the data being processed. (Article 15)
- ... have incorrect data corrected. (Article 16)
- ... have data erased. (Article 17)
Under GDPR, Data Subjects have the right to ...

- … know what’s going to be done with your data. (Article 13)
- … copies of all the data being processed. (Article 15)
- … have incorrect data corrected. (Article 16)
- … have data erased. (Article 17)
- … restrict processing. (Article 18)
Under GDPR, Data Subjects have the right to ...

- ... know what’s going to be done with your data. (Article 13)
- ... copies of all the data being processed. (Article 15)
- ... have incorrect data corrected. (Article 16)
- ... have data erased. (Article 17)
- ... restrict processing. (Article 18)
- ... data portability. (Article 20)
Under GDPR, Data Subjects have the right to ...

- ... know what’s going to be done with your data.  
  (Article 13)

- ... copies of all the data being processed.  
  (Article 15)

- ... have incorrect data corrected.  
  (Article 16)

- ... have data erased.  
  (Article 17)

- ... restrict processing.  
  (Article 18)

- ... data portability.  
  (Article 20)

- ... object to the data being processed.  
  (Article 21)
Under GDPR, Data Subjects have the right to …

- know what’s going to be done with your data. *(Article 13)*
- copies of all the data being processed. *(Article 15)*
- have incorrect data corrected. *(Article 16)*
- have data erased. *(Article 17)*
- restrict processing. *(Article 18)*
- data portability. *(Article 20)*
- object to the data being processed. *(Article 21)*
- not be subject to automated processing. *(Article 22)*
Under GDPR, Data Subjects have the right to...

- know what’s going to be done with your data.  
  (Article 13)
- copies of all the data being processed.  
  (Article 15)
- have incorrect data corrected.  
  (Article 16)
- have data erased.  
  (Article 17)
- restrict processing.  
  (Article 18)
- data portability.  
  (Article 20)
- object to the data being processed.  
  (Article 21)
- not be subject to automated processing.  
  (Article 22)

At no charge
Within 1 Month

Data Controller (or Processor) Responsibilities

20 articles that detail what a Data Controller and Data Processor must do.
Data Controllers must ...

... be accountable, demonstrate compliance (Article 24)
Data Controllers must ...

... be accountable, demonstrate compliance (Article 24)

... adopt privacy by design. (Article 25)
Data Controllers must ...

... be accountable, demonstrate compliance (Article 24)

... adopt privacy by design. (Article 25)

... if not in the EU, appoint a representative. (Article 27)
Data Controllers must ...

... be accountable, demonstrate compliance (Article 24)

... adopt privacy by design. (Article 25)

... if not in the EU, appoint a representative. (Article 27)

... take care when using third parties (Processors) (Article 28)
Data Controllers must ...

- be accountable, demonstrate compliance (Article 24)
- adopt privacy by design. (Article 25)
- if not in the EU, appoint a representative. (Article 27)
- take care when using third parties (Processors) (Article 28)
- keep records of processing. (Article 30)
Data Controllers must …

... be accountable, demonstrate compliance (Article 24)

... adopt privacy by design. (Article 25)

... if not in the EU, appoint a representative. (Article 27)

... take care when using third parties (Processors) (Article 28)

... keep records of processing. (Article 30)

... do security well. (Article 32)
Data Controllers must …

- be accountable, demonstrate compliance (Article 24)
- adopt privacy by design. (Article 25)
- if not in the EU, appoint a representative. (Article 27)
- take care when using third parties (Processors) (Article 28)
- keep records of processing. (Article 30)

- do security well. (Article 32)
- tell the regulator if they have a breach (72 hrs). (Article 33)
Data Controllers must ...

- be accountable, demonstrate compliance (Article 24)

- adopt privacy by design. (Article 25)

- if not in the EU, appoint a representative. (Article 27)

- take care when using third parties (Processors) (Article 28)

- keep records of processing. (Article 30)

- do security well. (Article 32)

- tell the regulator if they have a breach (72 hrs). (Article 33)

- tell Data Subjects about some breaches. (Article 34)
Data Controllers must ... 

- ... be accountable, demonstrate compliance (Article 24)
- ... adopt privacy by design. (Article 25)
- ... if not in the EU, appoint a representative. (Article 27)
- ... take care when using third parties (Processors) (Article 28)
- ... keep records of processing. (Article 30)

- ... do security well. (Article 32)
- ... tell the regulator if they have a breach (72 hrs). (Article 33)
- ... tell Data Subjects about some breaches. (Article 34)
- ... do privacy impact assessments. (Article 35,36)
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Article</th>
</tr>
</thead>
<tbody>
<tr>
<td>... be accountable, demonstrate compliance</td>
<td>(Article 24)</td>
</tr>
<tr>
<td>... adopt privacy by design.</td>
<td>(Article 25)</td>
</tr>
<tr>
<td>... if not in the EU, appoint a representative.</td>
<td>(Article 27)</td>
</tr>
<tr>
<td>... take care when using third parties (Processors)</td>
<td>(Article 28)</td>
</tr>
<tr>
<td>... keep records of processing.</td>
<td>(Article 30)</td>
</tr>
<tr>
<td>... do security well.</td>
<td>(Article 32)</td>
</tr>
<tr>
<td>... tell the regulator if they have a breach (72 hrs).</td>
<td>(Article 33)</td>
</tr>
<tr>
<td>... tell Data Subjects about some breaches.</td>
<td>(Article 34)</td>
</tr>
<tr>
<td>... do privacy impact assessments.</td>
<td>(Article 35,36)</td>
</tr>
<tr>
<td>... appoint a Data Protection Officer where specified.</td>
<td>(Article 37,38,39)</td>
</tr>
</tbody>
</table>
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 ...
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
Appropriate technical and organisational measures

- state of the art
- costs of implementation
- the nature, scope, context and purposes of processing

the risk of varying likelihood and severity for the rights and freedoms of natural persons
# Impact Assessment

- Financial impact
- Reputational impact
- Regulatory impact

## Impact to who?

**Impact to the organisation**

<table>
<thead>
<tr>
<th>Impact</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Negligible</td>
<td>Unlikely</td>
</tr>
<tr>
<td>Minor</td>
<td>Low</td>
</tr>
<tr>
<td>Significant</td>
<td>Medium</td>
</tr>
<tr>
<td>Critical</td>
<td>High</td>
</tr>
<tr>
<td>Certain</td>
<td>Certain</td>
</tr>
</tbody>
</table>
Appropriate technical and organisational measures

- state of the art
- costs of implementation
- the nature, scope, context and purposes of processing

the risk of varying likelihood and severity for the rights and freedoms of natural persons
(aka Data Subjects)
Impact on Data Subjects..

- Respect for private and family life, home and communications
- Physical and mental integrity
- Liberty and security of person
- Freedom of thought, conscience and religion
- Freedom of expression
- Protection of personal data
- Freedom to work and choose an occupation
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, including inter alia as appropriate:
including inter alia as appropriate:

amongst other things
a) the pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to **restore** the **availability** and **access** to personal data **in a timely manner** in the event of a physical or technical incident;
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
Security - summary

• Risk assess from the Data Subject's perspective
• Would use of pseudonymisation or encryption proportionately reduce the risk to Data Subjects?
• Don’t just concentrate in confidentiality
• What is the RTO – how would this affect a Data Subject?
• What’s the assurance framework – how do you know your controls are effective?
And what if an organisation chooses to ignore the GDPR?
<table>
<thead>
<tr>
<th>Lawful, fair and transparent</th>
<th>Expected by the person whose data it is</th>
<th>Just enough data to do what you’re doing</th>
<th>Accurate</th>
<th>Only kept as necessary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article 5(1)(a)</td>
<td>Article 5(1)(b)</td>
<td>Article 5(1)(c)</td>
<td>Article 5(1)(d)</td>
<td>Article 5(1)(e)</td>
</tr>
</tbody>
</table>

"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)."

Article 5(1)(f)

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 3 (‘accountability’)."

Article 5(2)
Complain to a supervisory authority (Article 77)

Administrative fines. €20M or 4% global turnover (Article 83)
Complain to a supervisory authority (Article 77)

Administrative fines. €20M or 4% global turnover (Article 83)

Complain to a court (Article 79)

Compensation for material or non-material damage (Article 82)

Data Subject

Solicitor representing a Data Subject

Not-for-profit body

Compensation for material or non-material damage

Administrative fines. €20M or 4% global turnover

Data Subject

Solicitor representing a Data Subject

Not-for-profit body

Compensation for material or non-material damage

Administrative fines. €20M or 4% global turnover
Complain to a supervisory authority (Article 77)

Administrative fines. €20M or 4% global turnover (Article 83)

Compensation for material or non-material damage (Article 82)

Data Subject
- know what’s going to be done with your data. (Article 13)
- copies of all the data being processed. (Article 15)
- have incorrect data corrected. (Article 16)
- have data erased. (Article 17)
- restrict processing. (Article 18)
- data portability. (Article 20)
- object to the data being processed. (Article 21)
- not be subject to automated processing. (Article 22)

Complain to a court (Article 79)

Solicitor representing a Data Subject (Article 80)

Not-for-profit body
Complain to a supervisory authority (Article 77)

Administrative fines. €10M or 2% global turnover (Article 83)

Compensation for material or non-material damage (Article 82)

Data Subject

Solicitor representing a Data Subject (Article 80)

Not-for-profit body (Article 80)
A note on penalties

It is unlikely that general (rather than serious and malicious) breaches of GDPR will result in the ‘top’ level of penalties.
Preparing for GDPR

Remember this is from an IT and Information Security perspective
Big picture

Does the regulation apply to us?
Big picture

Does the regulation apply to us?

Who are our Data Subjects

What and how much?
Big picture

Does the regulation apply to us?

Who are our Data Subjects

What and how much?

- Customers
- Workers

- Special category data (health, criminal etc.)
- Financial data
- How much?
Big picture

- Customers
- Workers

Does the regulation apply to us?

Who are our Data Subjects

- Special category data (health, criminal etc.)
- Financial data
- How much?

Catalog of systems and third parties

- Customers
- Workers
Big picture

• Customers
• Workers

Does the regulation apply to us?

Who are our Data Subjects
What and how much?

Catalogue of systems and third parties

• Special category data (health, criminal etc.)
• Financial data
• How much?

Regulatory organisational risk assessment
Regulatory risk assessment

Money no object
Playing Safe
Probably OK
Hope we’re lucky

2018 2019 2020
Create governance framework
1. Where is your data?

Create governance framework
1. Work out where personal data is

- Map data flows
- Be selective – work from high risk – low risk
- Logical and physical
- What do you store:
  - How old is it
  - How much is there
- What third parties?
1. Where is your data?

Create governance framework

Check all processing is fair, lawful and allowed
1. Where is your data?

Create governance framework

Check all processing is fair, lawful and allowed

Update policies and comms to data subjects
1. Where is your data?

Create governance framework

Check all processing is fair, lawful and allowed

Update policies and comms to data subjects

Appoint Data Protection Officer
1. Where is your data?
   - Create governance framework
   - Check all processing is fair, lawful and allowed
   - Update policies and comms to data subjects

2. Delete unwanted data.
   - Appoint Data Protection Officer
2. Delete all the data you don’t need

• Duplicate copies
• “Just-in-case” backups
• Excess fields in systems
• Records the business has decided is no longer required
1. Where is your data?
   - Create governance framework
   - Check all processing is fair, lawful and allowed
   - Update policies and comms to data subjects

2. Delete unwanted data.
   - Appoint Data Protection Officer

3. Do risk assessments
3. Do risk assessments

• Conduct security risk assessment
  • Effects of breach of CIA and R on data subject rights
  • (Article 32)

• Third party risks
  • (Article 28 & 44 if outside the EU)
1. Where is your data?
   - Create governance framework
   - Check all processing is fair, lawful and allowed
   - Update policies and comms to data subjects

2. Delete unwanted data.
   - Appoint Data Protection Officer

3. Do risk assessments
   - Processing outside the EU
1. Where is your data?
   - Create governance framework
   - Check all processing is fair, lawful and allowed
   - Update policies and comms to data subjects

2. Delete unwanted data.
   - Processing outside the EU
   - Appoint Data Protection Officer

3. Do risk assessments

4. Work out how to respond to Data Subject requests
4. Understand technically how to respond to ...

... know what’s going to be done with your data. (Article 13)

... copies of all the data being processed. (Article 15)

... have incorrect data corrected. (Article 16)

... have data erased. (Article 17)

... restrict processing. (Article 18)

... data portability. (Article 20)

... object to the data being processed. (Article 21)

... not be subject to automated processing. (Article 22)

1. Where is your data?
   - Create governance framework
   - Check all processing is fair, lawful and allowed
     - Update policies and comms to data subjects
     - Appoint Data Protection Officer

2. Delete unwanted data.
   - Processing outside the EU

3. Do risk assessments

4. Work out how to respond to Data Subject requests

5. Create risk register
   - Prioritise risk register
5. Create (& prioritise) privacy risk register

- List risks to Data Subjects
  - Prioritised
- List regulatory risks
  - Prioritised
  - Do and not do
  - There will be some non-compliant activities you have that are unlikely to have any impact on data subjects
1. Where is your data?
   - Create governance framework
     - Check all processing is fair, lawful and allowed
     - Update policies and comms to data subjects
   - Appoint Data Protection Officer

2. Delete unwanted data.

3. Do risk assessments
   - Processing outside the EU

4. Work out how to respond to Data Subject requests

5. Create risk register
   - Prioritise risk register

6. Plan and remediate
6. Risk reduction and remediation

• Do we need to do this with that data?
• Confidentiality
  • Pseudonymisation
  • Encryption
• Access control – does everyone need access?
• What security posture based on data subject risk
  • Will you create different security zones?
1. Where is your data?
   Create governance framework
   Check all processing is fair, lawful and allowed
   Update policies and comms to data subjects
   Appoint Data Protection Officer

2. Delete unwanted data.

3. Do risk assessments
   Processing outside the EU

4. Work out how to respond to Data Subject requests

5. Create risk register
   Prioritise risk register

6. Plan and remediate

7. DPIA for in-flight projects
7. DPIA for in-flight projects:

• DPIAs required for ‘high risk’ processing and in specified circumstances (Art 35):

• Needs to contain:
  • Systematic description and basis of processing
  • Assessment of necessity and proportionality
  • Risks to Data Subjects
  • Risk reduction

• Good practice

• Think of any InfoSec projects (DLP, monitoring) especially
1. Where is your data?
   - Create governance framework
   - Check all processing is fair, lawful and allowed
   - Update policies and comms to data subjects
   - Appoint Data Protection Officer

2. Delete unwanted data
   - Processing outside the EU

3. Do risk assessments
   - Prioritise risk register

4. Work out how to respond to Data Subject requests
   - 6. DPIA for in-flight projects

5. Plan and remediate
   - Create records of processing
Records of processing (Art 30)

- Essential for accountability principle
  - the purposes of the processing
  - a description of the categories of data subjects and of the categories of personal data
  - disclosure & recipients
  - where possible, the envisaged time limits for erasure of the different categories of data
  - where possible, a general description of the technical and organisational security measures
1. Where is your data?
   - Create governance framework
   - Check all processing is fair, lawful and allowed
     - Update policies and comms to data subjects
     - Appoint Data Protection Officer

2. Delete unwanted data

3. Do risk assessments
   - Processing outside the EU
   - 6. DPIA for in-flight projects

4. Work out how to respond to Data Subject requests
   - Create incident response plans

5. Create risk register
   - Prioritise risk register
   - 5. Plan and remediate
   - Create records of processing
What’s a personal data breach?

4(12) ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
Incident response

• Notification of a breach to supervisory authority within 72 hours (Art 33)
• Notification to Data Subject if high risk (Art 34)
• Plan, test the plan
• Make sure legal are involved (because they will want to handle the notification)
Plan for BAU
Integrating GDPR into IT BAU (esp. change)

- **Lawful, fair and transparent**
  - Article 5(1)(a)
  - ... be accountable, demonstrate compliance (Article 24)

- **Expected by the person whose data it is**
  - Article 5(1)(b)
  - ... adopt privacy by design. (Article 25)

- **Just enough data to do what you’re doing**
  - Article 5(1)(c)
  - ... take care when using third parties (Processors)

- **Only kept as long as necessary.**
  - Article 5(1)(e)
  - ... keep records of processing. (Article 30)

- **... do privacy impact assessments. (Article 35,36)**
  - ... do security well. (Article 32)

---

**At no charge**
**Within 1 Month**

- ... know what’s going to be done with your data. (Article 13)
- ... copies of all the data being processed. (Article 15)
- ... have incorrect data corrected. (Article 16)
- ... have data erased. (Article 17)
- ... restrict processing. (Article 18)
- ... object to the data being processed. (Article 20)
- ... not be subject to automated processing. (Article 22)
Change 1

• Check we have the right to do this with personal data
• Define minimum necessary data
• Set retention periods
• If copying data, how will it be updated?

• How will you support Data Subject rights – check each one

... know what’s going to be done with your data. (Article 13)
... copies of all the data being processed. (Article 15)
... have incorrect data corrected. (Article 16)
... have data erased. (Article 17)
... restrict processing. (Article 18)
... data portability. (Article 20)
... object to the data being processed. (Article 21)
... not be subject to automated processing. (Article 22)
Change 2

• Build privacy-by-design / data-protection by design into SSDLC

• Conduct Data Protection Impact Assessment (PIA)
  • Effects of processing on data subject rights

• Conduct security risk assessment
  • Effects of breach of CIA and R on data subject rights

• Third party risks

• Maintain documentation to demonstrate accountability
Your next steps

- Ignore Information Security vendors :-)
- Work out if the Regulation applies to you
- Big picture – Data Subjects and Risk
- Use the plan

- Think about BAU
Time for questions

(but remember I’m not a lawyer)