
Brexit and the Data
Protection Challenge

evolvenorth muckle LLP

Brexit and the Data Protection Challenge

Mark Dennis

Introductions and Agenda

evolve north

Introductions

Agenda

10.30am	Introductions	Mark Dennis - Evolve North
10.45am	Brexit and the Law	Stephanie Kyne – Muckle LLP
11.15am	Data Transfers	Helen McElroy – Evolve North
12.15 Lunch		
1.00pm	Practicalities	Mark Dennis – Evolve North
2.00pm	Technical Considerations	David Moffatt– Evolve North
2.30pm	Q+A and close	

Safety and facilities….
Please feel free to ask questions – there are no stupid questions….
Please feel free to stay after the event if you wish to discuss any specific issues…

en

evolvenorth

Introductions

What's the objective for today

- To try and clarify where the GDPR and Data Protection Act sit post Brexit
  - In respect to a no deal Brexit
  - In respect to a managed withdrawal
- To get all of you thinking about your or your clients data
  - How are you going to manage it post Brexit
  - What are the implications (if any)
- What actions might you need to take
  - Review of data
  - Review of processes
- Be prepared

en

Introductions

Evolve North

- What do we do….
  - Information Governance and IT Security working with GDPR, Data Protection Act, PCI DSS, ISO27001, NIS (National Infrastructure Security) Cyber Essentials and much more
- Who do we work with…
  - Financial Services, Hospitality, Political Parties, Building Society's, Ports, Airports, Legal and Law, Manufacturing, Marketing, NHS, Fire and Rescue, Football clubs, Retail, Rail and many more
- What's our approach….
  - Hands on practical - common sense driven
- What's our experience…
  - As a business over 15 years, as individuals over 20 years
  - In respect to data outside the EU……

"The superior man, when resting in safety, does not forget that danger may come. When in a state of security he does not forget the possibility of ruin. When all is orderly, he does not forget that disorder may come. Thus his person is not endangered, and his States and all their clans are preserved."

Confucius

evolve north

evolve north

muckle LLP

Brexit and Data Protection

Stephanie Kyne, Muckle LLP

en

Data Transfers – Next Steps

Helen McElroy
Senior Information Governance Manager

Understanding data transfers

- ICO Six Steps Guidance
- Two different types of transfer
  - Personal data coming into the UK
    - From the EU
      - Currently covered under GDPR
      - After Brexit – additional safeguards may be required
  - Personal data transferred out of the UK
    - New UK transfer and documentation provisions
- Organisations operating across Europe
  - DP regimes that apply (One Stop shops)
  - European representatives

Personal Data – out of the UK

Are you making restricted transfers? Yes if….

- UK GDPR doesn't apply to the organisation receiving the data (i.e. because they are located in a country outside the UK (which may be in the EU, the EEA or elsewhere)

Plus

- You and the receiver are separate organisations (even if you are both companies within the same group) *[not to consumers]*

Personal Data – out of the UK

Transfers from UK to EEA permitted

Gibraltar - fine

Not EEA – additional safeguards

Personal Data – into the UK

- On exit day – UK third party country
- Receiving a restricted transfer if you are located in the UK and an EEA located organisation sends you personal data
  - Cloud solution in EU
  - Service provider acting on your behalf in the EU
- EEA organisation will be able to make a restricted transfer to the UK with additional safeguards

Additional Safeguards

1. Adequacy decision made by the UK government
2. Appropriate safeguards
   i. Standard Contractual Clauses
   ii. Binding Corporate Rules
   iii. Public Bodies - Administrative Arrangement/Contract
   iv. Other safeguards (potentially)
3. Exceptions

Adequacy Decisions

- Adequate data protection regime in place
  - UK to recognise EU adequacy decisions prior to exit
  - But UK not seen as “adequate” currently for transfers in

- EU-US Privacy Shield Framework
  - Updated standards of compliance
  - Relevant organisation must have implemented updates

Appropriate Safeguards

Standard Contractual Clauses

- contract incorporating standard data protection clauses adopted by the Commission
- sets of standard contractual clauses for restricted transfers between a controller and controller, and two sets between a controller and processor

Binding Corporate Rules

- internal code of conduct operating within a multinational group
- restricted transfers of personal data from the group's EEA entities to non-EEA group entities.
- corporate group or a group of undertakings or enterprises engaged in a joint economic activity, such as franchises or joint ventures
- must submit BCRs for approval to an EEA supervisory authority in an EEA country where one of the companies is based

Public Bodies

- A legally binding and enforceable instrument between public authorities or bodies
- Administrative arrangements between public authorities or bodies which include enforceable and effective rights for the individuals, authorised by a
- supervisory authority

Exceptions

Exception 1 - Consent

- Has the individual given his or her explicit consent to the restricted transfer?

Exception 2 – Contract (Ind.)

- Do you have a contract with the individual?
- Is the restricted transfer necessary for you to perform that contract?
- Are you about to enter into a contract with the individual?
- Is the restricted transfer necessary for you to take steps requested by the individual in order to enter into that contract?

Exception 3 - Contract (other person)

- Do you have (or are you entering into) a contract with an individual which benefits another individual whose data is being transferred?
- Is that transfer necessary for you to either enter into that contract or perform that contract?

Exception 4 – Public Interest

- You need to make the restricted transfer for important reasons of public interest.
- EU/UK law implies importance

Exceptions

Exception 5 – Legal Claim

- You need to make the restricted transfer to establish if you have a legal claim, to make a legal claim or to defend a legal claim.

Exception 6 – Vital Interests

- You need to make the restricted transfer to protect the vital interests of an individual.
- He or she must be physically or legally incapable of giving consent.

Exception 7 – Public Register

- You are making the restricted transfer from a public register.

Exception 8 – Legitimate Interests

- Where no adequacy decision applies
- Cannot use other safeguard
- Not a regular transfer
- Only relating to limited individuals
- LIA
- ICO and individual informed

Summary

From:	To:	Measures required
UK	**EEA**	No additional measures required, UK recognises all EEA states as "adequate"
UK	**"Adequate" non-EEA country**	No additional measures required, UK will follow adequacy rulings by the EU on a transitional basis
UK	**Non-EEA country**	Existing rules apply (i.e. appropriate safeguard required) Standard contractual clauses can continue to be used or binding corporate rules or Privacy Shield
EEA	**UK**	No specific guidance on any requirements other than the law as it stands, meaning controllers based in the EEA would need to put in place one of the appropriate safeguards

One stop shop

- If carrying out cross-border processing, you benefit from the GDPR One-Stop-Shop system
- Single supervisory authority will act as the lead on behalf of the other EEA supervisory authorities
- Applies if you have an office, branch or other establishment in the UK and your processing is **likely to affect** individuals in one or more of the other EU or EEA states because:
  - You are processing the same set of personal data in the context of the activities of both your UK establishment and one or more EEA offices, branches, or other establishments.
  - You only have offices, branches or other establishments in the UK, but your processing of personal data is likely to substantially affect data subjects in one or more other EU or EEA states.
- Whether this will still apply after Brexit

European Representatives

Applicable to	After Brexit	Representative	Ensure that	Exceptions (where representative not needed)
• UK organisation not established in EEA, but offering goods or services to EEA individuals • UK organisation not established in EEA, but monitoring behaviour of EEA individuals	• UK no longer EEA based, so must appoint a representative in EEA	• Authorised in writing to act on your behalf to deal with supervisory authorities/data subjects • Examples - law firm, consultancy or private company (under service contract)	• Data subjects/supervisory authority can tell who this is – privacy notice, website etc • Located in one of the European countries that data subjects are from	• you are a public authority; or • your processing is only occasional, of low risk to the data protection rights of individuals, and does not involve special category or criminal offence data on a large scale

What to do now

Take stock

- Understand flows of personal data – will they become restricted transfers on exit date.
- Prioritise transfers for action
  - Transfers from EEA to UK
  - Large volumes of data
  - Special category data, criminal convictions and offences data
  - Business critical transfers

Additional measures

- How will you continue to make and receive those transfers lawfully after exit date
- Which appropriate safeguards will be in place

One-stop Shops/ European Reps

- Will need to deal with several supervisory authorities or not
- Will one-stop shops apply to you
- Will you need representatives in the EU

evolvenorth

Practicalities

Mark Dennis

Practicalities

This is an attempt…

To identify the practical steps you can take in respect to

- Your Data
- Policy and Procedure
- Third-parties
- Risk Management
- The Flipside

All feels a bit like GDPR 2.0….

Practicalities

Getting to know your data

Don't make assumptions…

About the location of your data

It is difficult to establish in many cases the physical location of your data

- Review your Information Asset Register – if you don't have one build one
- Add a column to your IAR to identify potential "third country" issues
- Raise issues to your Risk Register – if you don't have one build one
- When you start digging you may be surprised where your data actually resides…..

About how data flows

Review the flow of data

- Create simple data flow diagrams
- Particularly important if you process complex data

About third-parties

Identify third-parties you share data with (there will be more than you think)

- Including physical location
- Are they using further services to manage your data
- Where is their physical location i.e. where do they operate?

Practicalities

Getting to know your data

Some of the usual suspects

Practicalities

Getting to know your data

Where to look..

HR Systems
- Cloud based
- Third party management (outsourced)

Finance Systems
- Cloud based
- Third party management (outsourced)
- Payroll bureau services

CRM
- Cloud based
- Call centre locations

Marketing
- Cloud based
- Mails shots
- E marketing
- Surveys

The oddballs
- Legal support
- Overseas Agents
- Overseas entities of your business

Practicalities

Policy and Procedure

Review and update

Policy

Make sure it reflects the "third country" position

- Add references to third country data protection law if required
- Detail approach to managing data for third countries
- Recognise other Countries Data Protection Laws – Privacy Shield for example
- You may need to create "specific" Policy post Brexit

Procedure

Ensure it reflects the reality

- Review for third country data transfers
- Data sharing will need review
- Ensure you document these reviews

Training and Awareness

Make sure people know and understand that there are changes

- At board level awareness must be raised
- Staff should be made aware of changes and trained if required

Practicalities

Policy and Procedure

Review the components of your ISMS (information security management system)

Policy

Procedure

Training

Audit

IT Security

Practicalities

Third Parties

Don't make assumptions…..

Don't trust anyone – paranoia is your friend not your enemy!

Formalise your due diligence

- Structured questionaries'
- Request copies of policy and procedure
- Request certifications and ask for progress against ISO27001, Cyber Essentials
- Always, always establish if you need to do a DPIA (retrospective is more than acceptable)
- Establish location of data and operations

Top tips

If the response to your diligence is

- Slow, wordy, flowery light on documents – keep digging
- Quick, concise, positive and heavy on documents – keep digging (see first line above)
- In our experience, Big business does not always = good
- Small business, in our experience, does not always = bad

If you have any doubts, seriously consider

Site visits
Speak to the DPO/Responsible person directly

Practicalities

Third Parties

Your diligence should cover the following as a minimum

Policy

Procedure

Training

Audit

IT Security

Old Yorkshire saying – “I don’t trust anyone except me and thee an I'm not sure about thee”

Practicalities

Manage the risk

Be proactive…..

Think of it as a stick to beat people with

Risk Register

- A very useful tool for allocating a risk to an individual in a business, but more importantly ownership
- If its on the risk register its under control (to some extent)
- Use it to identify and manage risks with third parties

Visibility

Make sure the business

- Knows of the risks
- Understands the risks
- That there may be a financial cost to address some of these risks

DPIA (data protection impact assessments)

Forwards and backwards

- For new projects/relationships/systems – they work and without a doubt they help keep you safe
- For old projects/relationships/systems – they work very well retrospectively and if you have doubts use one

Practicalities

Manage the risk

> "Risk mitigation is painful, (and) not a natural act for humans to perform"
>
> Gentry Lee | NASA Jet Propulsion Lab

Sums it up – but we need to do it

Practicalities

The Flip Side

Meeting the needs of others – current experience

Once outside the EU

Other people/organisations will be

- Wanting a lot more evidence about your compliance with GDPR, Data Protection Act etc.
- Looking for third party validation/checking of you compliance (ISO, Cyber Essentials, FCA)
- Expecting you to provide documented evidence

You may need to create additional documents

For example

- ISMS Overview
- Profiles and qualifications/experience of DPO (Data Protection Officer) IT Security Manager
- Sharing vulnerability/penetration testing outputs

You may need to consider additional certifications

- ISO27001
- ISO9001
- Cyber Essentials

Practicalities

The Flip Side

Things that help

CYBER ESSENTIALS PLUS

Information Security Management System ISO 27001 Certified

bsi. ISO 9001:2015 Quality Management

NIS Directive

Vulnerability Assessment

password
****
strength

TP Penetration Testing

Practicalities

Timescales

Option 1 No deal Brexit - 42 working days

Option 2 Managed Withdrawal - 520 working days

Practicalities

Questions

Assuming you have all not lost the will to live……

Please remember –

- We will always answer questions and try and provide guidance
- We are happy to share document templates
- If it all goes wrong we will always try and help

evolvenorth

Technical Considerations

David Moffatt

evolvenorth

Maintain the Basics

No requirement for bleeding-edge technology

Don’t ignore development in security solutions – they’re always going to be reacting to changing attack techniques

Make sensible decisions when selecting your solutions and technologies and document your reasons for choosing them

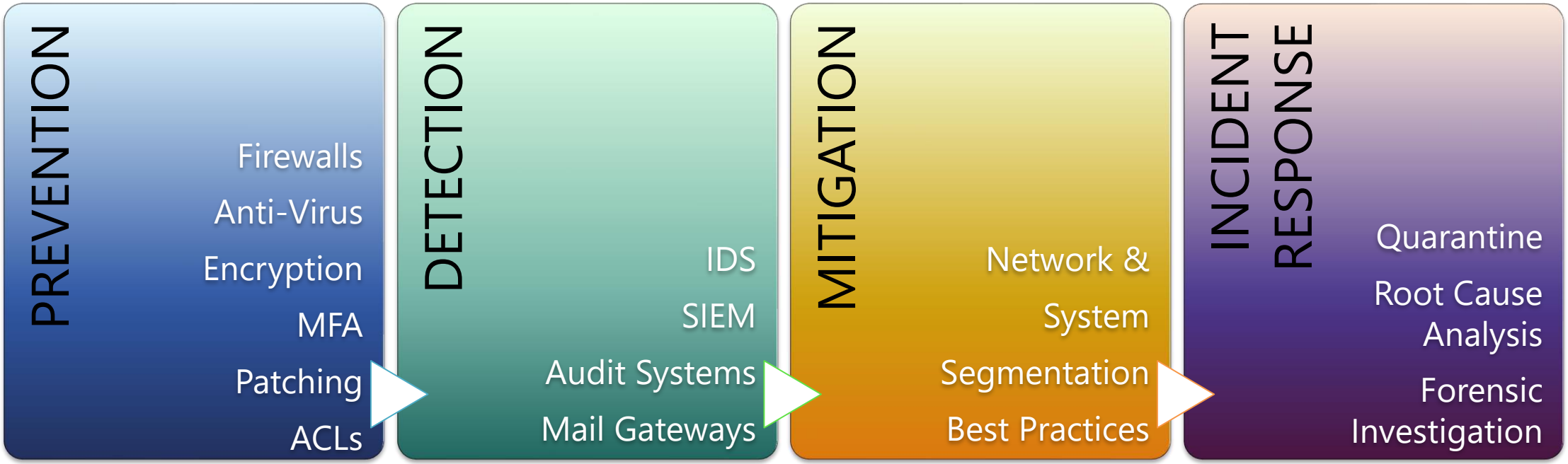
Ensure that concepts such as Role-Based Access and Least Privilege are used throughout all systems

en

evolvenorth

IT Security Best Practice

Four Core Concepts of IT Security



evolve north

Encryption

Protect your Data at Rest

- Ensure high-risk devices (laptops, tablets, smartphones) are all protected
- Also consider desktops and servers

Data in Transit

- Update systems to support latest cryptographic protocols (TLS 1.3)
- Disable support for “broken” and legacy versions (SSL 3.0, TLS1.1…)

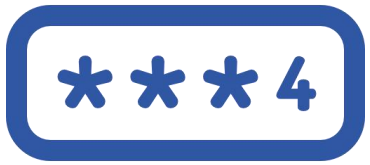
en

evolvenorth

Multi-Factor Authentication

MFA

- Username and Password is not enough
- Protects against account compromise
- Simple to implement
- Easy to use



evolvenorth

Vulnerability Scanning

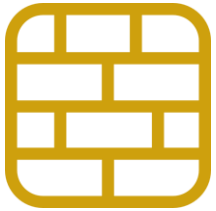
Carry out regular vulnerability scans

- External Infrastructure – Quarterly at a minimum
  - Published Websites
  - Externally Accessible Resources (OWA, File Transfer, Remote Access)
- Internal Infrastructure – Ongoing or at frequent intervals

en

evolvenorth

Penetration Testing



More involved than Vulnerability Scanning

- Carry out on an annual basis
- Internal Infrastructure
- External Infrastructure
- Private Cloud Environments
- Publicly Accessible Infrastructure
- Wireless Environments

Use an agreed framework and methodology (OWASP, NIST…)

- Verify scope of the assessment covers all necessary areas
- Ensure results are documented, risk assessed and actioned

en

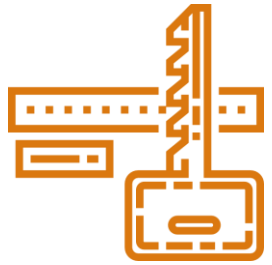
evolvenorth

Password Auditing

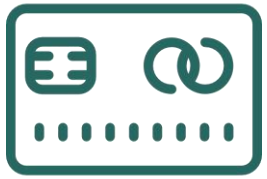
Passwords remain as the most critical element to protect your business

Password Audit:

- Evaluates the effectiveness of your Password Policy
- Highlights areas of risk
- Demonstrates how quickly weak passwords can be cracked



Combine with User Education to improve password strength and complexity



en

evolvenorth

To find out more:

www.evolvenorth.com

01748 905 002 | info@evolvenorth.com


Thank you