



EU DATA PROTECTION

CHANGES TO LAW AND HOW ARCHER CAN HELP

RSA


What is this all about?

- The EU is in the process of reforming its existing data protection rules.
- These reforms have been moving slowly through the EU legislative pipeline but we seem now to be getting closer to a final agreement. Even though the expected implementation date of these rules is still likely to be two years away it is strongly recommend that businesses prepare now as the reforms go well beyond an upgrade.
- Archer can really help businesses to not only plan ahead but implement effective measures.





What is EU Data Protection?

- ▶ The right to privacy is mainly regulated in the EU under a 1995 Directive that controls the processing of personal data. These rules are of very wide effect with major compliance requirements placed on businesses inside and outside the EU
- ▶ Personal data can include:
 - ▶ Individual's name, age, home address, race, sexual orientation, income, health, blood type, marital status, education, and employment information
 - ▶ And many more.....
 - ▶ This applies to everyone



What is *personal* data



- **Personal data** relates to a living individual who can be identified:
 - (a) from those data, or
 - (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,
 - and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

MK99 – Big Data

8

So about these changes....

- Are they completely new rules?
 - Yes and No
 - Yes – The 1995 rules are being completely replaced
 - No - Not only will the fundamental aspects of privacy continue to be protected, they will also be extended.

What new rules will there be?

- There are in fact two proposed sets of new rules as follows:
 - Firstly, there is a Regulation, which sets out a general EU framework for data protection, i.e. to replace the 1995 Directive. A Regulation has been chosen because this format should be immediately applicable law once adopted. Further, Member States like the UK will still face legislative issues about what to do with aspects of their national data protection rules that are additional to the EU rules.
 - Secondly, there is a Directive, which specifically deals with protecting personal data processed in a law enforcement context.

Continued....

- Additionally
 - A key aspect of the reforms is that a business which is in several EU Member States should only have to deal with one data protection regulator (called a “supervisory authority” in the Regulation) – Though this presents issues....
 - Cross-Border data protection
 - Lack of current local DPA co-operation + ‘ego’
 - Judicial challenges

My business is not in the EU.....

- The new rules will apply not only to businesses which are actually located in an EU Member State, but, also, to businesses located completely outside the EU where they process the personal data of EU residents and offer them goods and services, which the June 2015 Council text qualifies as being “irrespective of whether a payment by the data subject [the person concerned] is required”. This extra-territorial dimension is a very significant change and very controversial. A key issue is that it may prove very difficult, if not impossible, to actually enforce this.

What will customers need to do?

- ▶ Thoroughly review vendor contracts – customers will need vendors' help especially in reporting privacy breaches very quickly. They will make sure they have the contracts to insist on this and will need to hold vendors to account;
- ▶ Implement a subject access request procedure. It can be used to deal with right to be forgotten requests. A good subject access request process will reduce compliance risks and act as an early warning radar for other issues in the business.
- ▶ Put in place a data breach notification procedure, including notification and response capabilities – considering special insurance

- ▶ Prepare to update processes and prepare new documentation and records ready for regulatory inspection;
- ▶ Review all key processes such as data retention, destruction through all means of collecting data from the business;
- ▶ Ensure that new policies such as explicit consent, the right to be forgotten, right of data portability and erasure, the right to not be subject to profiling are included in policies and procedures
- ▶ Put in place a Privacy Impact Assessment (PIA) process (most customers should be doing this anyway!!).
- ▶ Set up and undertake regular compliance audits in order to identify and rectify issues

Example: Data Breaches

- There are two reporting obligations. Significant changes concerning the mandatory reporting of data breaches are to be introduced.
- Data breaches will have to be reported to data protection regulators in each country affected without delay and, where possible, not later than a period to be set under the new rules, which in the November 2015 Council text is set at 72 hours
- . The notification to the regulator will have to be accompanied by a reasoned justification in cases where it is not made within the set period.
- This does not seem likely to be a one stop shop system, so, for example if you have a breach affecting 12 EU countries you will likely have to make 12 separate reports within the 24 or 72 hours allowed.



Two particular contentious issues that may prove a challenge are:

- Whether there will be a threshold, i.e. if a breach is minor whether it will have to be notified or not.
- Whether technical measures to secure the data, such as encryption, will mean that a breach need not be reported and if so what those acceptable technical measures will be. This is important for multinationals as US data breach laws commonly provide exceptions for data which is sufficiently encrypted.



“Data protection fines are nothing to be scared of, it’s not like anti-competition.....”

- Under the new rules, data protection regulators will have the power to impose high fines for infringing the data rules
- Three different bands of fines are proposed in relation to three different categories of infringements
- This could be around 1m Euro or up to 2% of the global annual turnover of a business, whichever is the greater, in the highest category of the three bands and infringements



HOW CAN ARCHER BENEFIT OUR CUSTOMERS?

Stages of Breach Submission



Enroll in Workflow

Date Created: 1/21/2016 5:55 PM Last Updated: 1/21/2016 7:24 PM

BREACH INFORMATION

Breach ID: DB-2

Date of Breach: 1/20/2016 12:00 AM

Date Reported: 1/21/2016 5:52 PM

Date Closed:

Days Open: 0

Status: New

Breach Type: Personal Information Breach

Breach Submitter: Breach Submitter 1

Priority: Medium

Discovery Method: Int - Reported by user

Breach Details: An employee has given to a third party the login and password for an account with global access rights to the client database. Using this account, the third-party can access all the customer information without any restrictions. The database includes name, address, email, phone numbers, access and other identifying data (user name, hashed passwords, customer ID) as well as payment data (account number, credit card details, etc.). Even though payment data was encrypted with a state of the art algorithm, the master account compromised was authorised to access it, thus the third party also had access. The company has more than 100.000 customers.

Policy Breached				Add New Lookup	
Policy Name		Policy Statement			
Personal Data Security Breach Policy		This policy deals with protecting personal data processed in a law enforcement context. It ensures that new aspects such as explicit consent, the "right to be forgotten", "right of data portability" and erasure, and the right to not be subject to profiling.			
Country:	<div>Germany</div> <div>United Kingdom</div>	...	Edit	Regulatory Authority:	<div>Germany Officer</div> <div>United Kingdom Officer</div>

General

ASSIGNMENT

Breach Owner: Chahine, Yasser

Breach Manager: Officer, DP

Notify Breach Owner: No, do not send an email notification to the breach owner.

Additional Access:

Estimated Hours: 48

DATA INFORMATION

Data Encrypted: Yes

Encryption Details: AES (Advanced Encryption Standard)

Impacted Information Assets: Customer Information Database

Customer Data: Yes

Customer Data Details: Personal Customer Information

HISTORY LOG

Notification to Internal Stakeholders

Subject: Policy DP-01: Personal Data Security Breach

The logo for RSA Archer eGRC, featuring the word "RSA" in white on a red square background, followed by "Archer eGRC" in white text on a grey background.

Hello Team,

Please note that Policy [DP-01: Personal Data Security Breach Policy](#) has been breached.

Click the link below to access the record:

<https://archer/default.aspx?requestUrl=..%2fGenericContent%2fRecord.aspx%3fid%3d579067%26moduleId%3d657>

Thanks,

Archer Admin

The logo for RSA Archer eGRC, featuring the word "RSA" in white on a red square background, followed by "Archer eGRC" in white text on a grey background.

Date Created: 1/21/2016 5:55 PM Last Updated: 1/21/2016 7:24 PM

BREACH INFORMATION

Breach ID:	DB-2	Status:	New	Edit
Date of Breach:	1/20/2016 12:00 AM	Breach Type:	Personal Information Breach	Edit
Date Reported:	1/21/2016 5:52 PM	Breach Submitter:	Breach Submitter 1	Add
Date Closed:		Priority:	Medium	Edit
Days Open:	0	Discovery Method:	Int - Reported by user	Edit
Breach Details:	An employee has given to a third party the login and password for an account with global access rights to the client database. Using this account, the third-party can access all the customer information without any restrictions. The database includes name, address, email, phone numbers, access and other identifying data (user name, hashed passwords, customer ID) as well as payment data (account number, credit card details, etc.). Even though payment data was encrypted with a state of the art algorithm, the master account compromised was authorised to access it, thus the third party also had access. The company has more than 100,000 customers.			

Policy Breached

Add New | Lookup |

Policy Name	Policy Statement
Personal Data Security Breach Policy	This policy deals with protecting personal data processed in a law enforcement context. It ensures that new aspects such as explicit consent, the "right to be forgotten", "right of data portability" and erasure, and the right to not be subject to profiling.
Country:	Regulatory Authority:
Germany	Germany Officer
United Kingdom	United Kingdom Officer

General

ASSIGNMENT

Breach Owner:	Chahine, Yasser	Notify Breach Owner:	<input type="radio"/> Yes, send an email notification to the breach owner.
			<input checked="" type="radio"/> No, do not send an email notification to the breach owner.
Breach Manager:	Officer, DP		Edit
		Additional Access:	
		Estimated Hours:	48

Risks

Add New | Lookup |

Risk	Description
Data Theft	The organization does not have the capability to manage accounts giving access to internal systems leading to poor data protection lack of non-repudiation or accountability.

Control Standards

Add New | Lookup |

Standard Name
Data retention & destruction

Control Procedures

Add New | Lookup |

Procedure Name
Privacy Impact Assessment process
Regular Compliance Audits

Breach Tasks

Add New | Lookup |

Breach Task ID	Task Name
No Records Found	

Notification of Breach Rejection

Subject: Data Breach DB-2 has been rejected

The logo for RSA Archer eGRC, featuring the word "RSA" in white on a red square background, followed by "Archer eGRC" in white text on a grey background.

Hello Team,
Please note that Data Breach [DB-2](#) has been rejected with the following Comments:

The data breach mentioned in the subject line does not violate the Policy [DP-01](#): Personal Data Security Breach Policy.

Click the link below to access the record:

<https://archer/default.aspx?requestUrl=.%2fGenericContent%2fRecord.aspx%3fid%3d579062%26moduleId%3d37>

Thanks,
DP Officer

The logo for RSA Archer eGRC, featuring the word "RSA" in white on a red square background, followed by "Archer eGRC" in white text on a grey background.

Date Created: 1/21/2016 5:55 PM Last Updated: 1/21/2016 7:24 PM

BREACH INFORMATION

Breach ID:	DB-2	Status:	New	Edit
Date of Breach:	1/20/2016 12:00 AM	Breach Type:	Personal Information Breach	Edit
Date Reported:	1/21/2016 5:52 PM	Breach Submitter:	Breach Submitter 1	Add
Date Closed:		Priority:	Medium	Edit
Days Open:	0	Discovery Method:	Int - Reported by user	Edit
Breach Details:	An employee has given to a third party the login and password for an account with global access rights to the client database. Using this account, the third-party can access all the customer information without any restrictions. The database includes name, address, email, phone numbers, access and other identifying data (user name, hashed passwords, customer ID) as well as payment data (account number, credit card details, etc.). Even though payment data was encrypted with a state of the art algorithm, the master account compromised was authorised to access it, thus the third party also had access. The company has more than 100,000 customers.			

Policy Breached		Add New Lookup	
Policy Name	Policy Statement		
Personal Data Security Breach Policy	This policy deals with protecting personal data processed in a law enforcement context. It ensures that new aspects such as explicit consent, the "right to be forgotten", "right of data portability" and erasure, and the right to not be subject to profiling.		
Country:	Germany United Kingdom	Regulatory Authority:	Germany Officer United Kingdom Officer

General

ASSIGNMENT

Breach Owner:	Chahine, Yasser	Notify Breach Owner:	<input type="radio"/> Yes, send an email notification to the breach owner. <input checked="" type="radio"/> No, do not send an email notification to the breach owner. Edit
Breach Manager:	Officer, DP	Additional Access:	
		Estimated Hours:	48

Risks	Add New Lookup	
Risk	Description	
Data Theft	The organization does not have the capability to manage accounts giving access to internal systems leading to poor data protection lack of non-repudiation or accountability.	

Control Standards	Add New Lookup	
Standard Name		
Data retention & destruction		

Control Procedures	Add New Lookup	
Procedure Name		
Privacy Impast Assessment process		
Regular Compliance Audits		

Breach Tasks	Add New Lookup	
Breach Task ID	Task Name	
No Records Found		

Notification to Control Owner

Subject: Data Breach DB-2 has been assigned to you for approval



Hello Team,

Please note that Data Breach [DB-2](#) has been assigned to you for approval.

Click the link below to access the record:

<https://archer/default.aspx?requestUrl=..%2fGenericContent%2fRecord.aspx%3fid%3d579062%26moduleId%3d37>

Thanks,
DP Officer





BREACH INFORMATION

Date Created: 1/21/2016 5:55 PM Last Updated: 1/21/2016 7:24 PM

Breach ID: DB-2

Date of Breach: 1/20/2016 12:00 AM

Date Reported: 1/21/2016 5:52 PM

Date Closed:

Days Open: 0

Status: New

Breach Type: Personal Information Breach

Breach Submitter: Breach Submitter 1

Priority: Medium

Discovery Method: Int - Reported by user

Breach Details: An employee has given to a third party the login and password for an account with global access rights to the client database. Using this account, the third-party can access all the customer information without any restrictions. The database includes name, address, email, phone numbers, access and other identifying data (user name, hashed passwords, customer ID) as well as payment data (account number, credit card details, etc.). Even though payment data was encrypted with a state of the art algorithm, the master account compromised was authorised to access it, thus the third party also had access. The company has more than 100,000 customers.

Policy Breached

Policy Name: Personal Data Security Breach Policy

Policy Statement: This policy deals with protecting personal data processed in a law enforcement context. It ensures that new aspects such as explicit consent, the "right to be forgotten", "right of data portability" and erasure, and the right to not be subject to profiling.

Country: Germany, United Kingdom

Regulatory Authority: Germany Officer, United Kingdom Officer

General Resolution

ASSIGNMENT

Breach Owner: Chahine, Yasser

Breach Manager: Officer, DP

Notify Breach Owner: Yes, send an email notification to the breach owner. No, do not send an email notification to the breach owner.

Additional Access:

Estimated Hours: 48

Risks

Risk: Data Theft

Description: The organization does not have the capability to manage accounts giving access to internal systems leading to poor data protection lack of non-repudiation or accountability.

Control Standards

Standard Name: Data retention & destruction

Control Procedures

Procedure Name: Privacy Impact Assessment process, Regular Compliance Audits

Breach Tasks

Breach Task ID: No Records Found

Task Name:

DATA INFORMATION

Data Encrypted: Yes

Encryption Details: AES (Advanced Encryption Standard)

Customer Data: Yes

Customer Data Details: Personal Customer Information

Impacted Information Assets: Customer Information Database

HISTORY LOG

▼ RESULTS

Breach Result: Resolved - Allegation Confirmed ▼ Edit

Breach Resolution Detail: Breach for personal information has occurred, User account has been suspended.

Cause: Employee shared system credentials with the customer

Corrective Actions: Training employees on current policies.

▼ DATA INFORMATION

Data Encrypted: Yes ▼ Edit

Encryption Details: AES (Advanced Encryption Standard)

Customer Data: Yes ▼ Edit

Customer Data Details: Personal Customer Information

Impacted Information Assets: Customer Information Database ✕ ... Add

► HISTORY LOG

Report for Germany

Subject: Data Breach DB-2 has been reported

Hello Team,
Please note that Data Breach [DB-2](#): has been reported for Policy [DP-01](#): Personal Data Security Breach Policy

Breach details as follows:

Date of Breach: 1/20/2016 12:00 AM

Date Reported: 1/21/2016 5:52 PM

Date Closed: 1/22/2016 7:32 AM

Breach Type: Personal Information Breach

Priority: Medium

Discovery Method: Int - Reported by user

Breach Details: An employee has given to a third party the login and password for an account with global access rights to the client database. Using this account, the third-party can access all the customer information without any restrictions. The database includes name, address, email, phone numbers, access and other identifying data (user name, hashed passwords, customer ID) as well as payment data (account number, credit card details, etc.). Even though payment data was encrypted with a state of the art algorithm, the master account compromised was authorized to access it, thus the third party also had access. The company has more than 100.000 customers.

Country: Germany

Resolution:

Breach Result: Resolved - Allegation Confirmed

Breach Resolution Detail: Breach for personal information has occurred, User account has been suspended.

Cause: Employee shared system credentials with a third party.

Corrective Actions: Training employees on current policies.

Click the link below to access the record:

<https://archer/default.aspx?requestUrl=.%2fGenericContent%2fRecord.aspx%3fid%3d579062%26moduleId%3d37>

Thanks,

DP Officer

Report for United Kingdom

Subject: Data Breach DB-2 has been reported

Hello Team,
Please note that Data Breach [DB-2](#) has been reported for Policy [DP-01](#): Personal Data Security Breach Policy

Breach details as follows:

Date of Breach: 1/20/2016 12:00 AM

Date Reported: 1/21/2016 5:52 PM

Date Closed: 1/22/2016 7:32 AM

Breach Type: Personal Information Breach

Priority: Medium

Discovery Method: Int - Reported by user

Breach Details: An employee has given to a third party the login and password for an account with global access rights to the client database. Using this account, the third-party can access all the customer information without any restrictions. The database includes name, address, email, phone numbers, access and other identifying data (user name, hashed passwords, customer ID) as well as payment data (account number, credit card details, etc.). Even though payment data was encrypted with a state of the art algorithm, the master account compromised was authorized to access it, thus the third party also had access. The company has more than 100.000 customers.

Country: United Kingdom

Resolution:

Breach Result: Resolved - Allegation Confirmed

Breach Resolution Detail: Breach for personal information has occurred, User account has been suspended.

Cause: Employee shared system credentials with a third party.

Corrective Actions: Training employees on current policies.

Click the link below to access the record:

<https://archer/default.aspx?requestUrl=.%2fGenericContent%2fRecord.aspx%3fid%3d579062%26moduleId%3d37>

Thanks,
DP Officer

 Archer eGRC

Thank You – Any Questions?