GDPR
&
Mauritian Financial Services Business

Mathew Beale - Comsure

GDPR for non EU Companies

In addition to applying to businesses established in the EU, the EU General Data Protection Regulation (GDPR) also applies to businesses which are not established in the EU but which process personal data in relation to:

- The offering of goods or services to individuals in the EU (including free of charge), or
- Monitoring the behaviour of individuals in the EU

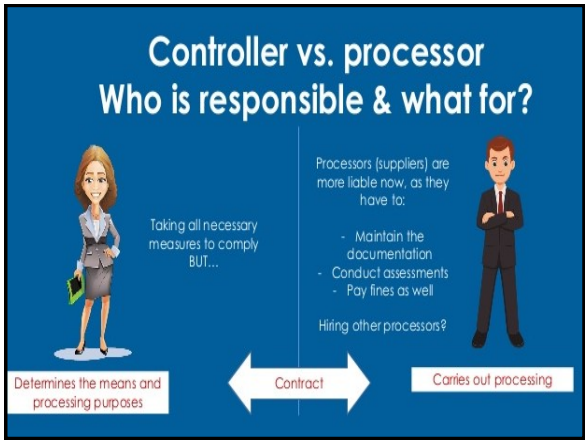
Summary video

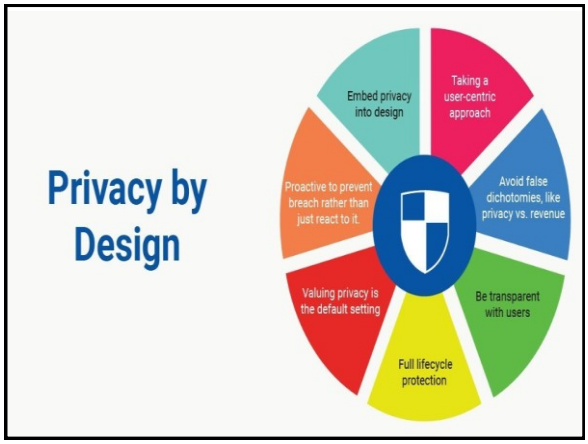
Data Subjects

Comsure

Comsure

Controllers and Processors





Comsure

Privacy by design to force controllers and processors to think about privacy and data protection (and security) from the start to the end of any processing activity and at all levels of responsibility within an organisation.

PERSONAL DATA

Comsure

Expansion of the definition of **PERSONAL DATA** to include **MORE CATEGORIES** of data within its scope. These include

1. **ANY INFORMATION** relating to an **IDENTIFIABLE PERSON** who can be **directly or indirectly** identified in particular by reference to an identifier
   - Name, **identification numbers**, location, **online identifiers,** etc.

2. **'SENSITIVE PERSONAL DATA'** data consisting of
   1. racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

6 REASONS

Introduction of further limitations or additional conditions on some legal grounds for **PROCESSING DATA** (which largely remain the same). These include

Lawful processing:

1. **Explicit consent of the data subject**
2. **Necessary for the performance of a contract**
3. **Necessary for legitimate interests**
4. Necessary for legal or judicial reasons
5. Necessary to protect the data subject's best interests
6. Necessary to perform a task carried out in the public interest

72-HOUR DATA BREACH NOTIFICATION (from its detection).

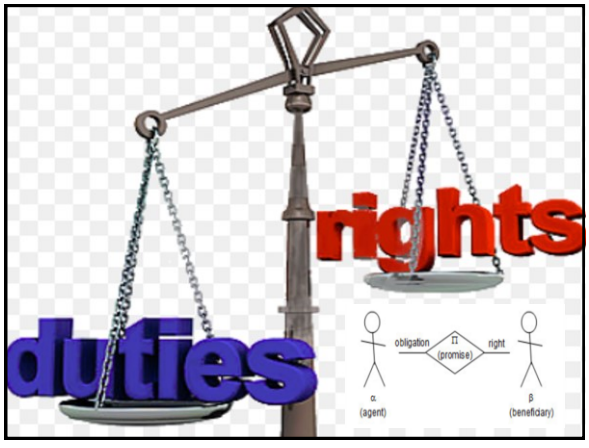
In cases where a breach poses a high risk to the data subjects, they will need to be notified 'without undue delay.'

DPO

Mandatory **DATA PROTECTION OFFICER** (DPO) for public authorities or bodies and where the organisation's core activities involve:

- a) regular and systematic monitoring of data subjects on a large scale or
- b) large scale processing of special categories of data and/or data relating to criminal offences.

The DPO must have sufficient expert knowledge of data protection law, and should act independently and report to the highest level of management.



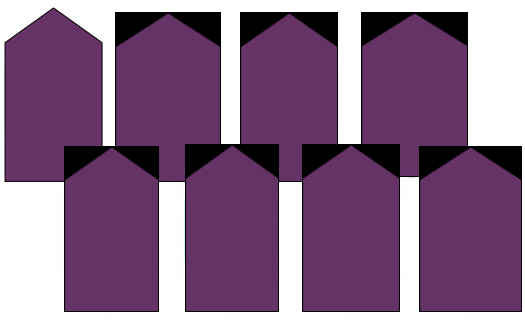
Comsure

The 8 Rights of the Data Subject [identified or identifiable natural person (‘data subject’)]

The data subject has a number of rights over their personal data and as an organisation we must ensure that we provide the mechanisms to allow them to exercise these rights.

These include:

What are the Data Subject Rights?

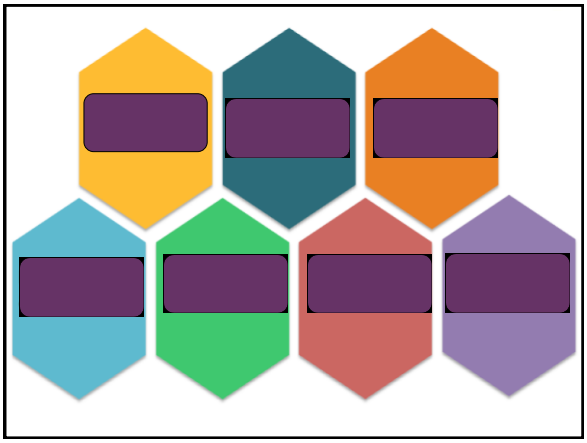


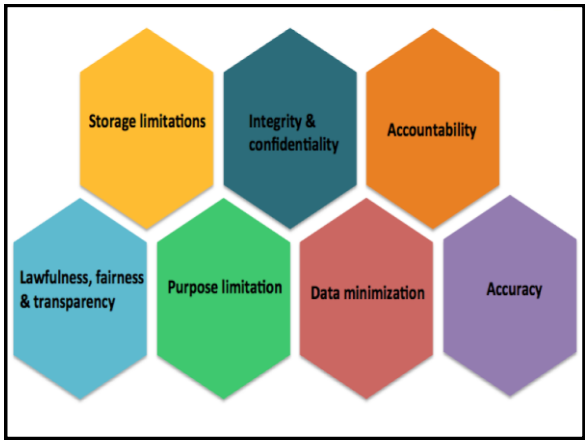
What are the Data Subject Rights?

Comsure

The 6 Privacy Principles (obligations)

When collecting and processing personal data we must abide by the six principles shown on the NEXT SLIDE:





International Data Transfers

Comsure

1. **Only** transfer personal data to countries deemed "adequate" by the EU
2. **Safeguards must** be agreed and in place **prior to transfer**
3. **Binding Corporate Rules** may be used within an international organization
4. **EU-US** transfers subject to separate agreement

Safeguards are deemed to be in place due to GDPR

When transferring data between EU AND European Free Trade Association (EFTA) countries the necessary safeguards are deemed to be in place due to GDPR –

The EU / EFTA countries are:

31

EU =

- Austria, Belgium, Bulgaria, Croatia, Republic of Cyprus, Czech Republic, Denmark, Estonia, Finland, France,
- Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta,
- Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the UK.

EFTA =

- Norway, Liechtenstein and Iceland

Also personal data can flow from the EU to a third country without any further safeguard being necessary where the EU has given equivalent status.

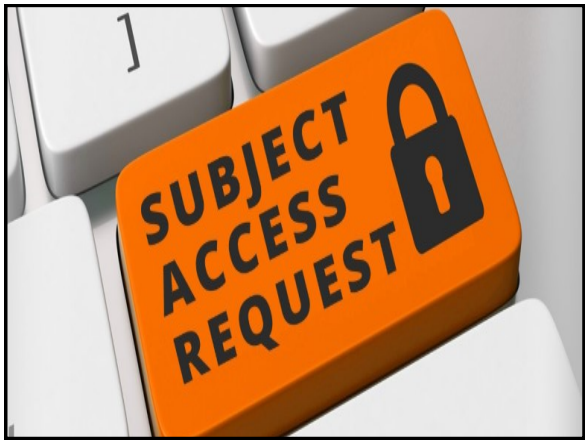
The European Commission has so far recognised

12

1. Andorra,
2. Argentina,
3. Canada (commercial organisations),
4. Faroe Islands,
5. Guernsey,
6. Israel,
7. Isle of Man,
8. Jersey,
9. New Zealand,
10. Switzerland,
11. Uruguay and
12. The US (limited to the Privacy Shield framework) as providing adequate protection.

Ensure you have privacy notices in place, which are clear and concise and set out all the information required under the GDPR, including

1. your contact details,
2. the purpose of the processing,
3. the period for which data will be stored,
4. the rights of data subjects
5. etc..



D-sars

Comsure

The rules on subject access requests will change:

1. You will have **one month** to comply subject to a two-month extension
2. You will not be able to charge a fee unless the request is manifestly unfounded, excessive or repetitive or if the data subject has requested further copies
3. The information will usually need to be provided In a commonly used electronic form

Comsure

GDPR for non EU Companies

GDPR for non EU Companies

For non-EU companies, the first step is therefore to assess whether you fall within the regime?

GDPR for non EU Companies

Once you have determined whether the GDPR applies to any part(s) of your business, steps need to be taken to comply

Whilst the exact make-up of your compliance programme will in part be unique to your business, to assist you Comsure have set out a number of actions Comsure suggest you consider taking.

As a minimum

In any event given the size of the task, Comsure suggests you prioritise actions based on appropriate factors for your business, including:

GDPR for non EU countries

1. How business critical an item is;
2. Whether an item needs to be dealt with now to future proof your business;
3. Whether / how easy temporary mitigation is;
4. The level of risk, and degree, of potential non-compliance;
5. The level of risk of regulator action, claims from individuals or reputational damage;
6. The business benefits of change, such as with customers and employees; and
7. The cost and time to implement change.

3 core areas

Preliminary actions
Customer facing
Internal operations and procedures.

Preliminary Steps

Preliminary Steps

Comsure

Board buy-in

Obtain the support of your board to the additional resources the compliance programme will need, whether this be monetary resource, for instance to update IT systems, or people resource from other parts of the business.

Preliminary Steps

Comsure

Governance and reporting structure

As with any project, an appropriate governance structure will need to be established to ensure appropriate reporting and engagement at each stage of the programme with the right people.

Preliminary Steps

Comsure

Data Audit

Run a personal data audit.

At a minimum, this should cover what personal data you collect, the uses of such data, to whom, and where, it is transferred and the security measures applied to it.

Preliminary Steps

Comsure

Gap Analysis

Using the information from the data audit, perform a gap analysis to identify areas where changes are required.

This will help inform the rest of your DPR compliance programme.

Comsure

Customer Facing Areas

Lawful processing:

Comsure

1. **Explicit consent of the data subject**
2. **Necessary for the performance of a contract**
3. **Necessary for legitimate interests**
4. Necessary for legal or judicial reasons
5. Necessary to protect the data subject's best interests
6. Necessary to perform a task carried out in the public interest

Customer Facing Areas

Comsure

Privacy By Design

Consider how privacy by design can be introduced into your business to meet the specific requirements of the GDPR, as well as to assist you with complying with the general accountability requirements.

Customer Facing Areas

Comsure

Sensitive Personal Data

Identify if you process genetic or biometric data as these are now categorised as sensitive personal data.
If so, put in place now processes to obtain explicit consent.

Customer Facing Areas

Comsure

Sensitive personal data is a specific set of "special categories" that must be treated with extra security.

These categories are:

1. Racial or ethnic origin;
2. Political opinions;
3. Religious or philosophical beliefs;
4. Trade union membership;
5. Genetic data; and
6. Biometric data (where processed to uniquely identify someone).

Customer Facing Areas

Comsure

Child consent

If you rely on consent from children in the context of digital services, check whether your processes comply with the requirements of the GDPR and if not, change them now in order to future proof your processing.

Customer Facing Areas

Comsure

Automated processing and profiling

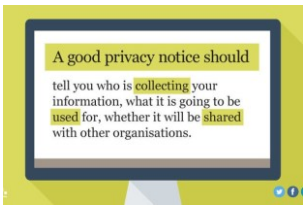
Analyse whether any automated processing you undertake, such as profiling, produces legal effects concerning the individual or similarly significantly affects them as consent will then be required.

Customer Facing Areas

Comsure

Privacy Notices

Review your privacy notices to determine if they meet the new content requirements and the general requirements as to transparency and clarity of communication.



Customer Facing Areas

Comsure

Purpose limitation

Put in place processes to:

1. Identify any potential additional purposes of the processing at the outset; and
2. To check the basis for any additional purpose identified later on, so that personal data is not processed for additional purposes unless compliant with the GDPR requirements.

Comsure

Internal Operations and Procedures

Internal Operations and Procedures

Comsure

Commercial Contracts

New processor contracts:

1. ensure the provisions reflect that data processors have direct obligations under the GDPR,
2. the revised mandatory provisions for contracts with processors; and
3. the new breach notification requirements, as well as the consequential commercial impacts of the GDPR changes.

Existing processor contracts:

1. amend to reflect mandatory provisions.

Internal Operations and Procedures

Comsure

Anonymisation

Check whether anonymised data will meet the more stringent requirements for anonymisation.

It is the process of either encrypting or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous (Pseudonymisation).

If not, determine if these requirements can be met and analyse the implications of falling within the GDPR regime

Internal Operations and Procedures

Comsure

Insurance

Check the terms of any relevant insurance policies to determine if any changes are needed.

Internal Operations and Procedures

Comsure

Demonstrating compliance

Consider how best to demonstrate compliance. Whilst written policies and processes will be important, relying on long unwieldy documents that are not read or followed in practice will be insufficient.

Internal Operations and Procedures

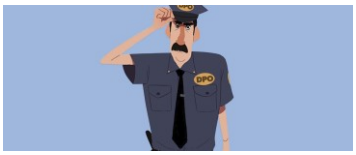
Supervisory Authority Audit

Put in place appropriate procedures for an audit or exercise of a warrant by your supervisory authority.

Internal Operations and Procedures

Data protection officer (DPO)

Determine whether you fall within the mandatory DPO regime and, if so, how best to integrate this function into your organisation.



Internal Operations and Procedures

Central data processing record

Ensure that you have a central record of all processing of personal data which contains the mandatory information under the GDPR.

Your data audit and completion of the rest of your compliance programme should assist in populating the required information.

Internal Operations and Procedures

Comsure

Data Privacy Impact Assessments (DPIAs)

Introduce processes to ensure that DPIAs are used where mandated by the GDPR and

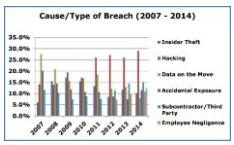
decide and implement your policy for broader usage as this will assist with complying with the general accountability requirements of the GDPR.

Internal Operations and Procedures

Comsure

Data breach

Put in place a comprehensive data breach reporting procedure and test it works operationally to allow compliance with the GDPR notification requirements.



Internal Operations and Procedures

Comsure

Data erasure, portability and restriction on processing

Put in place appropriate procedures to be able to comply with requests from individuals to erase, transfer or restrict the processing of personal data.

Internal Operations and Procedures

Comsure

Subject Access Requests (SARs)

Put in place processes to meet the requirements of the regime.

Internal Operations and Procedures

Comsure

Lead supervisor

If you have an establishment in the EU, determine the location of your main establishment and hence who your lead supervisory authority is.

Internal Operations and Procedures

Comsure

Training

Ensure everyone who has access to personal data receives appropriate training on the GDPR.

Comsure

1. Decide if you need to appoint a Data Protection Officer ('DPO').
2. Carrying out a data audit
3. Limit (Destroy) data – if you do not need it don't save it
4. Draw a data map
5. Data Subject Access Requests (dSAR)
6. Get Straight on Security – e.g. encryption
7. Privacy Notices
8. company policies
9. Staff Training
10. Privacy Impact Risk Assessments
11. Reporting data breaches
12. Dealing with contracts

Comsure

Summary and Closing Remarks

Comsure

Comsure

FINISH
ANY QUESTIONS...?

managing the **risks**
so you can focus
on the **rewards**

- **Comsure** was founded in 2005 with a view to providing comprehensive business **risk advisory services & is able to offer** your organisation a wealth of **skills and experience.**

Comsure

managing the **risks**
so you can focus
on the **rewards**

Mathew Beale

Email:

mathewbeale@comsuregroup.com

Tel:

01534 626841

Risk warning:

The information contained in this briefing is intended to provide Comsure delegates with a brief update in relation to the topics covered. The information and opinions expressed in this briefing do not purport to be definitive or comprehensive and are not intended to provide professional advice.

Comsure (and their associates and subsidiaries) are not responsible for, and do not accept any responsibility or liability in connection with, the content discussed during this briefing.