

  
Comsure



**GDPR**

## GENERAL DATA PROTECTION REGULATION

### How GDPR applies in Jersey

Address GDPR **FEAR** with compliant **FACT**

**18<sup>th</sup> May 2017**

8:15am to 12:30pm

**Pomme D'Or Hotel**



**6 x C.I. GDPR Surgery Workshops**

*monthly from Sep 2017 to Feb 2018*

[www.comsuregroup.com/gdpr-information](http://www.comsuregroup.com/gdpr-information)

**B E D E L L  
C R I S T I N**



 **LOGICALIS**  
Business and technology working as one

# Table of Contents

<b>News &amp; Workshops .....</b>	<b>2</b>
News .....	2
Chairmans thoughts.....	2
Events & Workshops .....	2
<b>C.I. GDPR Programme Itinerary .....</b>	<b>3</b>
<b>The Board &amp; GDPR .....</b>	<b>4</b>
Board/Management Questions.....	4
The view from the GDPR Authorities.....	4
<b>Business Benefits of GDPR .....</b>	<b>5</b>
<b>C.I. GDPR Timeline .....</b>	<b>6</b>
Time is now short within UK.....	6
Time is shorter within the C.I.....	6
<b>C.I. GDPR Surgery Programme .....</b>	<b>7</b>
Why you should attend the C.I. GDPR Surgeries.....	7
Article 29 Working Party 2017 Action Plan.....	7
C.I. GDPR Legal Status.....	7
GDPR Surgery Workshops: Proposed Dates.....	7
Surgery 1: The GDPR Compliance Roadmap .....	8
Surgery 2: Legal obligations & regulatory considerations.....	8
Surgery 3: Data management methodologies .....	9
Surgery 4: Right-sized data security obligations & tools.....	9
Surgery 5: Data risk mitigation, assurance & insurance .....	10
Surgery 6: GDPR Compliance Checklist & GAP.....	10
<b>GDPR Resources .....</b>	<b>11</b>

## News & Workshops

### News

The recent Ransomware storm, impacting the NHS and many others, provides a timely reminder of how best practice 'applied' (the prevention) is so much less disruptive and costly than the measures required to fix an issue that should never have existed (the cure).

- A news broadcast interview of one NHS Trust management spokes-person; when asked how the issue could be resolved, stated "we may have to pay the ransom".
  - Demonstrating that many senior managers and executives are willing to finance crime or terrorism rather than suffer data loss!
  - Yet those same 'execs' see no benefit from investment in data protection by default and design (at much lower cost) to protect their prime asset: the end client?

### Leadership thoughts

#### Tone from the top ...

- The Group CEO states "I appreciate our compliance team; but they need to be flexible. Our relationship/sales team deliver the business that keeps us employed!"

Do you ...

- Assess all enterprise risks in a balanced manner, through all levels of enterprise business lines, and then issue a risk assessed and departmentally qualified report - within 24 hours of the CEO's statement?

NO?

Perhaps you should ... Read on ...

### Events & Workshops

We have several workshops in a jurisdiction near you (and your 3rd parties).

Subscribe to Comsure: 'GDPR Surgery Workshops'

Subscribe to Comsure: V-CO, the ultimate regulatory 'One Source' protection

## C.I. GDPR Programme Itinerary

<b>8: 15 AM Registration</b>	
	Breakfast buffet
<b>8:45 AM Comsure Welcome &amp; Introduction</b>	
	<p><b>Mathew Beale:</b> Summary of the GDPR (C.I.) and the support available from the Comsure GDPR (C.I.) Surgery workshops.</p> <p><b>Paul Declat:</b> The new Chairman of Comsure Group discusses the power best practice delivers to sustainable business growth.</p>
<b>9:00 AM Office of the Information Commissioner</b>	
	<b>Emma Martins:</b> How GDPR applies in the Channel Islands & why it is good for C.I. businesses to exceed & excel.
<b>9:30 AM Bedell Cristin</b>	
	<b>Edward Drummond:</b> How GDPR will affect the law on data protection and information governance and what businesses should be thinking about now.
<b>10:00 AM KPMG</b>	
	<b>Andrei Voinescu:</b> How to apply a proportionate and scaleable GDPR compliance method for the enterprise or SME.
<b>10:30 AM Refreshments</b>	
<b>11:00 Data2Vault</b>	
	<b>Mark Saville:</b> Efficient and proportionate risk mitigation, assurance and insurance; what the directors should be considering at their next board meeting.
<b>11:30 AM Logicalis</b>	
	<b>Ricky Magalhaes:</b> Efficient security and privacy measures; practices required to achieve and maintain GDPR compliance, a reliable framework for PII and more.
<b>12:00 PM Questions</b>	
	12:30 PM Close

## The Board & GDPR

### Board/Management Questions

- A) Is the General Data Protection Regulation (GDPR) a threat or an opportunity for my business?
- B) How does the GDPR impact other regulations, specifically in relation to the C.I. international financial services industry focus?
- C) Can the GDPR improve sustainability and growth for C.I. businesses?

### The view from the GDPR Authorities

#### Building trust in the online environment is key to economic development

"Strong, reliable, consistently applied rules will make data processing safer, cheaper and inspire people's confidence. Confidence in turn drives growth. This is a message that is well understood worldwide. In a letter to the European Parliament strongly supporting the data protection reform package, 25 major US consumer organizations stressed that **"stronger privacy standards in Europe will benefit consumers around the globe"**.

#### Boost growth and encourage the flow of data

**"Sharing data has become crucial for economic growth.** Privacy protection and the free flow of data are complementary not contradictory concepts".

#### Allow business to get on with doing what it does best

**"Businesses operating globally will benefit from clear rules** that set out how they can use binding corporate rules (BCRs) and standard contractual clauses to transfer personal data securely. The proposal also abolishes many cumbersome prior-authorization procedures. Under certain conditions, it will be possible to transfer data outside the Union on the basis of codes of conduct".

Source: EU Factsheet 'Mythbusting'

#### The Islands are well positioned to leverage global reputation

"The Channel Islands are recognised world-wide for high standards of compliance; we are also 2 of the 9 territories outside the EU to have EU Adequacy. This creates a significant opportunity for the C.I. to build on past successes and reputation to ensure a strong and exciting future for our international industries".

Source: Emma Martins, the Information Commissioner of Jersey & Guernsey

## Business Benefits of GDPR

**General Notice:** The following list has been compiled by **Comsure** Group. It is derived from the ongoing review of GDPR publications from the sources cited below.

**C.I. Notice:** Some of the publications are subject to change, specifically in the Channel Islands where relevant laws are in the process of being drafted.

**Sources** (web site links provided on the **Resources** page):

- The Official Journal of the EU and The EU Article 29 Working Party on GDPR
- the UK Information Commissioners Office (ICO),
- the Jersey Office of the Information Commissioner (OIC), and
- the Guernsey Office of the Data Protection Commissioner (ODPC).

Business Benefits	Operational Benefits
<b>Single Standard</b>	simplified legal requirements & reduced administration
<b>Improved Security</b>	reduced business risk & increased business protection
<b>Improved Privacy</b>	strengthens client relationship & business retention
<b>Improved Trust</b>	growth of digital business & increased business opportunity
<b>Enhanced Efficiency</b>	reduced time & cost of doing business
<b>Explicit Best Practice</b>	reduced ambiguity & subjectivity
<b>Objective Evidence</b>	reduced compliance, criminal & civil action risks
<b>Traceable Liability</b>	increased counter-party control & reduced counter-party risk
<b>Holistic Regulation</b>	commensurable with other business regulations
<b>SME Optimised</b>	flexible measures & exemptions appropriate for SME's
<b>International Reach</b>	creates a level playing field & reduces unfair competition
<b>Protects Individuals</b>	management, personnel & client rights equally protected

# C.I. GDPR Timeline

## Time is now short within UK

The GDPR count-down started April 2016, when it was adopted into law within the EU (pre-BREXIT), and subsequently confirmed by UK Parliament in 2016 (post BREXIT).

## Time is shorter within the C.I.

The Channel Islands (Jersey/Guernsey) have agreed to apply a unified C.I. version of the GDPR within local law. The published deadline for ratification of the C.I. GDPR law is May 2018, while the earliest drafts of the C.I. laws are expected after summer 2017.

Therefore C.I. businesses will need a mechanism to ensure they are fully informed about the progress of the C.I. GDPR law, including guidance on the implications of the drafts as they come available, specifically regarding financial services regulation considerations.

**Beware: C.I. GDPR is not 'fixed' until ratified by C.I. law**

C.I. GDPR GANT Chart															
Q2 2017			Q3 2017			Q4 2017			Q1 2018			Q2 2018			
Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	
Awareness & Communication															
	C.I. GDPR	Comsure Advisory	Comsure GDPR C.I. Surgery Workshops										Regulation Date <b>25th May 2018</b>		
		Data Assessment & Plan	Update Contracts, Notices & Consents												
		Comsure Advisory	Define Policies & Procedures												
			GAP & Risk Audit	Training						Comsure Advisory					
			Implement Business & Technology Changes										Comsure Advisory		

## C.I. GDPR Surgery Programme

### Why you should attend the C.I. GDPR Surgeries

The GDPR has been published and accepted into EU and UK law in Q2 2016 as a complete regulation. However, the GDPR does not come into force until 25th May 2018 in order to allow interested groups to present objections/changes to the EU Article 29 Working Party.

The GDPR, as at Q2 2017, is not 100% complete and there are changes that may (or may not) be announced throughout 2017.

### Article 29 Working Party 2017 Action Plan

The 2017 Action Plan includes the following key elements:

**Completion of 2016 Work.** The Working Party will finalize its work, begun in 2016, in relation to (1) certification mechanisms, (2) high-risk processing, (3) Data Protection Impact Assessments, (4) administrative fines, (5) the implementation of the European Data Protection Board and (6) the implementation of the one-stop-shop and the consistency mechanisms.

**New 2017 Priorities.** The Working Party intends to publish guidelines on the following GDPR topics in 2017: (1) consent and profiling and (2) transparency. In addition, the Working Party also intends to update its existing referentials and opinions that relate to (1) data transfers to third countries and (2) data breach notification.

### C.I. GDPR Legal Status

Jersey and Guernsey have agreed to a unified C.I. GDPR law. The drafting process will be carried out throughout 2017. However, the deadline for completion is May 2018.

The C.I. GDPR Surgery Workshops allow attendees to be informed and enabled to adapt to change through 2017/18.

### GDPR Surgery Workshops: Proposed Dates

**Proposed dates (to be confirmed). The proposed subjects:**

Thursday 21 September 2017	The GDPR Compliance Roadmap
Thursday 19 October 2017	Legal obligations & regulatory considerations
Thursday 16 November 2017	Data management methodologies
Tuesday 12 December 2017	Right-sized data security obligations & tools
Thursday 25 January 2018	Data risk mitigation, assurance & insurance
Thursday 22 February 2018	GDPR Compliance Checklist & GAP

## Surgery 1: The GDPR Compliance Roadmap

<b>Host</b>	Comsure Group
<b>Location</b>	TBA: 40 attendee capacity
<b>Objectives</b>	<ol style="list-style-type: none"> <li>1. Issue the GDPR Handbook</li> <li>2. GDPR Handbook Section One:             <ol style="list-style-type: none"> <li>a) GDPR Roadmap (ICO 12-step programme) &amp; Milestones,</li> <li>b) General support materials &amp; resources</li> <li>c) GDPR tools review</li> </ol> </li> <li>3. How to complete a GDPR Benchmark Assessment (self-assessment &amp; independent assessment options) &amp; Action Plan,</li> <li>4. Panel introduction: roles &amp; resources,</li> <li>5. Prep for Surgery 2: Legal obligations &amp; regulatory considerations</li> </ol>

## Surgery 2: Legal obligations & regulatory considerations

<b>Host</b>	Bedell Cristin
<b>Location</b>	TBA: 40 attendee capacity
<b>Objectives</b>	<ol style="list-style-type: none"> <li>1. Publish GDPR updates</li> <li>2. GDPR Handbook Section Two:             <ol style="list-style-type: none"> <li>a) GDPR currently defined legal obligations &amp; 'watch-list' threats, specifically relating to other regulatory/legal considerations,</li> <li>b) Legal support materials, sample T&amp;C's/Notices &amp; resources</li> <li>c) Legal methods of deleting PII data</li> <li>d) Example Binding Corporate Agreement (BCA)</li> </ol> </li> <li>3. How to complete a Legal Benchmark Assessment (self-assessment &amp; independent assessment options) &amp; Legal Action Plan,</li> <li>4. Panel discussion: regulatory precedence &amp; legal 'pot-holes',</li> <li>5. Prep for Surgery 3: Data management methodologies</li> </ol>

### Surgery 3: Data management methodologies

<b>Host</b>	(TBA, KPMG)
<b>Location</b>	TBA: 40 attendee capacity
<b>Objectives</b>	<ol style="list-style-type: none"> <li>1. Publish GDPR updates</li> <li>2. GDPR Handbook Section Three:             <ol style="list-style-type: none"> <li>a) GDPR currently defined data privacy obligations &amp; 'watch-list' threats, specifically relating to C.I.,</li> <li>b) Compare GDPR methods for Enterprises &amp; SME's,</li> <li>c) Define GDPR Enterprise vs SME criteria</li> </ol> </li> <li>3. Panel discussion: enterprise data privacy, including 3rd parties</li> <li>4. Prep for Surgery 4: Right-sized data security obligations &amp; tools</li> </ol>

### Surgery 4: Right-sized data security obligations & tools

<b>Host</b>	Logicalis
<b>Location</b>	TBA: 40 attendee capacity
<b>Objectives</b>	<ol style="list-style-type: none"> <li>1. Publish GDPR updates</li> <li>2. GDPR Handbook Section Four:             <ol style="list-style-type: none"> <li>a) GDPR currently defined data security measures &amp; obligations, with 'watch-list' threats specifically relating to C.I.,</li> <li>b) Data security methods &amp; tools; how to identify solutions for your business size and type,</li> </ol> </li> <li>3. How to complete a Data Security Assessment (self-assessment &amp; independent assessment options) &amp; Data Security Action Plan,</li> <li>4. Panel discussion: enterprise data security, including internal &amp; external threats</li> <li>5. Prep for Surgery 5: Data risk mitigation, assurance &amp; insurance</li> </ol>

## Surgery 5: Data risk mitigation, assurance & insurance

<b>Host</b>	Data2Vault
<b>Location</b>	TBA: 40 attendee capacity
<b>Objectives</b>	<ol style="list-style-type: none"> <li>1. Publish GDPR updates</li> <li>2. GDPR Handbook Section Five:             <ol style="list-style-type: none"> <li>a) GDPR currently defined data risk mitigation measures &amp; standards, with 'watch-list' threats specifically relating to C.I.,</li> <li>b) Data risk mitigation support materials, example risk mitigation &amp; control methods &amp; resources,</li> <li>c) How 'Data Audit' reduces residual risk (insurance) costs.</li> </ol> </li> <li>3. How to complete a Data Risk Assessment (self-assessment &amp; independent assessment options) &amp; Risk Mitigation Action Plan,</li> <li>4. Panel discussion: enterprise data risks best practice, including internal &amp; external treatments &amp; controls</li> <li>5. How to prepare for Surgery 6: GDPR Compliance Checklist &amp; GAP</li> </ol>

## Surgery 6: GDPR Compliance Checklist & GAP

<b>Host</b>	Comsure Group
<b>Location</b>	TBA: 40 attendee capacity
<b>Objectives</b>	<ol style="list-style-type: none"> <li>1. Publish GDPR updates</li> <li>2. GDPR Handbook Section Six:             <ol style="list-style-type: none"> <li>a) GDPR checklist &amp; best practice standards, with GAP analysis &amp; outstanding risk exposure specifically relating to C.I.,</li> <li>b) Compliance 'fast-track' support materials, methods &amp; resources,</li> <li>c) GAP identification &amp; resolution methods/resources</li> </ol> </li> <li>3. How to complete a Compliance GAP Assessment (self-assessment &amp; independent assessment options) &amp; Corrective Action Plan,</li> <li>4. Panel discussion: GDPR Compliance &amp; ongoing monitoring</li> </ol>

## GDPR Resources

### **Comsure Group & Certified Training**

[www.comsuregroup.com/gdpr-information](http://www.comsuregroup.com/gdpr-information)

### **The Jersey Office of the Information Commissioner**

<https://dataci.je>

### **Bedell Cristin**

<https://www.bedellcristin.com>

### **KPMG**

<https://home.kpmg.com/qm/en/home.html>

### **Data2Vault**

<http://www.data2vault.com>

### **Logicalis**

<http://www.je.logicalis.com>

### **EU GDPR**

[http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm)

[http://ec.europa.eu/newsroom/just/news.cfm?tpa\\_id=2026](http://ec.europa.eu/newsroom/just/news.cfm?tpa_id=2026)

<http://www.eugdpr.org/more-resources-1.html>

### **UK Information Commissioners Office**

<https://ico.org.uk>

### **Other reputable resources**

[www.Galaxkey.com](http://www.Galaxkey.com)

[www.DynaRisk.com](http://www.DynaRisk.com)