General Data Protection Regulation

The new EU General Data Protection Regulation (GDPR) introduces significant changes to the EU data protection regime, designed to strengthen and unify data protection for individuals across Europe. GDPR comes into force on the 25th of May 2018.

Aurexia CONSULTING

PARIS | LONDON | LUXEMBOURG | HONG-KONG | SINGAPORE

STRATEGY & MANAGEMENT CONSULTING

March, 2018

Overview of the key changes under GDPR

General Data Protection Regulation – Aurexia Consulting

Increased Territorial Scope

Apply to the processing of personal data of data subjects residing in the Union by controllers and processors in the EU, regardless of whether the processing takes place in the EU or not;

Data Protection Officers

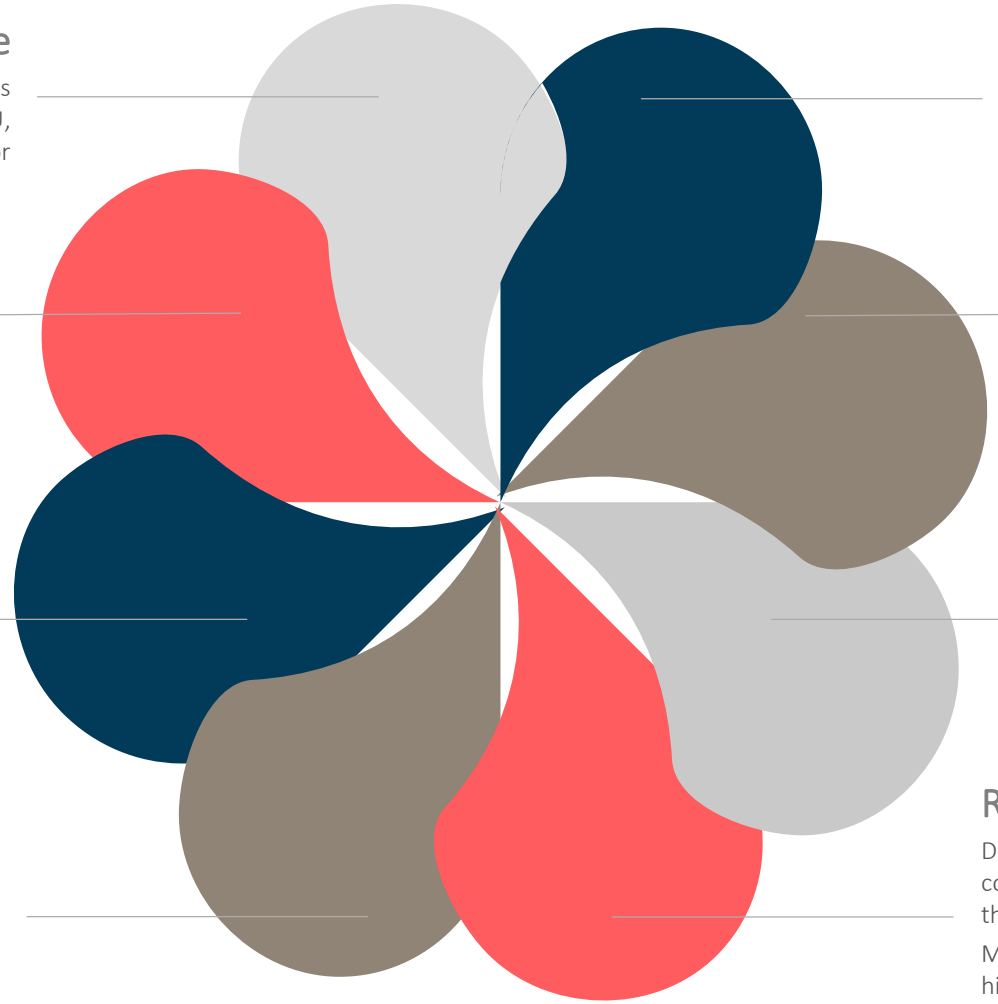
DPO appointment will be mandatory only for those controllers and processors whose core activities consist of processing operations which require regular and systematic monitoring of data subjects on a large scale or of special categories of data or data relating to criminal convictions and offences;

Privacy by design

"The controller shall..implement appropriate technical and organisational measures..in an effective way.. in order to meet the requirements of this Regulation and protect the rights of data subjects" Art.23;

Data Portability

The right for a data subject to receive the personal data concerning them, which they have previously provided in a 'commonly use and machine readable format' and have the right to transmit that data to another controller;



Penalties

(maximum fine) up to 4% of annual global turnover or €20 Million - not having sufficient customer consent to process data or violating the core of Privacy by Design concepts;

Consent

The request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent;

Breach Notification

In all member states where a data breach is likely to "result in a risk for the rights and freedoms of individuals" breach notification must be done within 72 hours of first having become aware of the breach;

Right to Access & Right to be forgotten

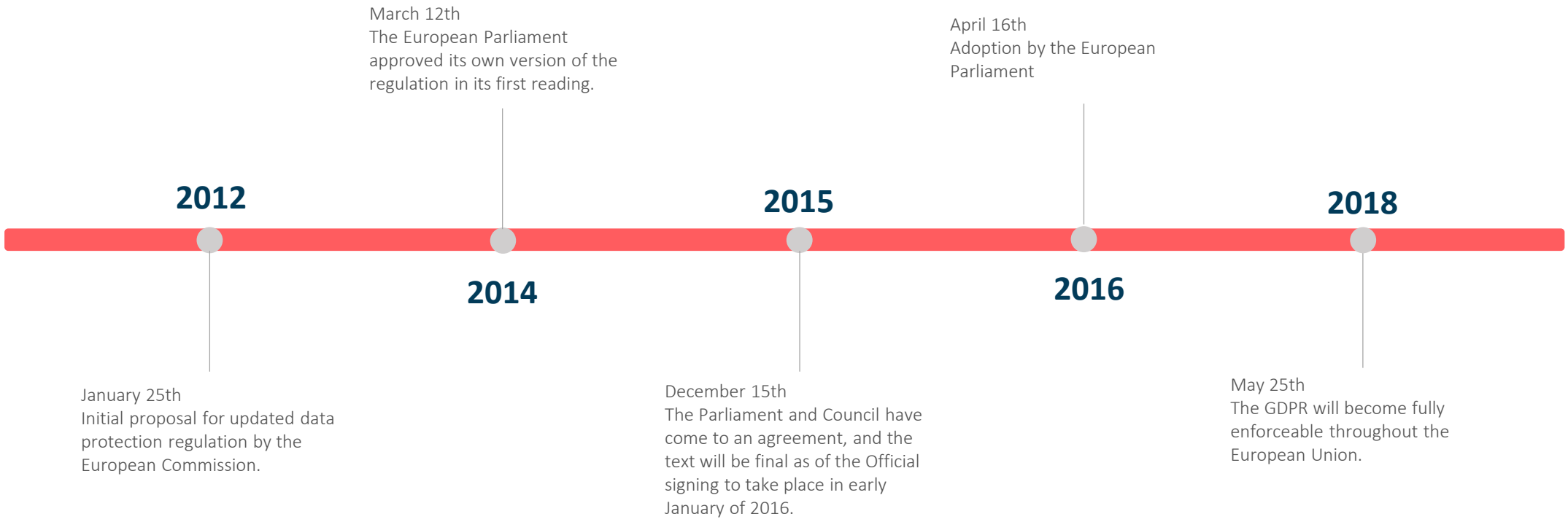
Data subjects have the right to obtain from the data controller confirmation as to whether or not personal data concerning them is being processed, where and for what purpose;

Moreover, data subjects can have the data controller erase his/her personal data, and potentially have third parties halt processing of the data;

Aurexia CONSULTING

GDPR Timeline

General Data Protection Regulation – Aurexia Consulting



Aurexia CONSULTING

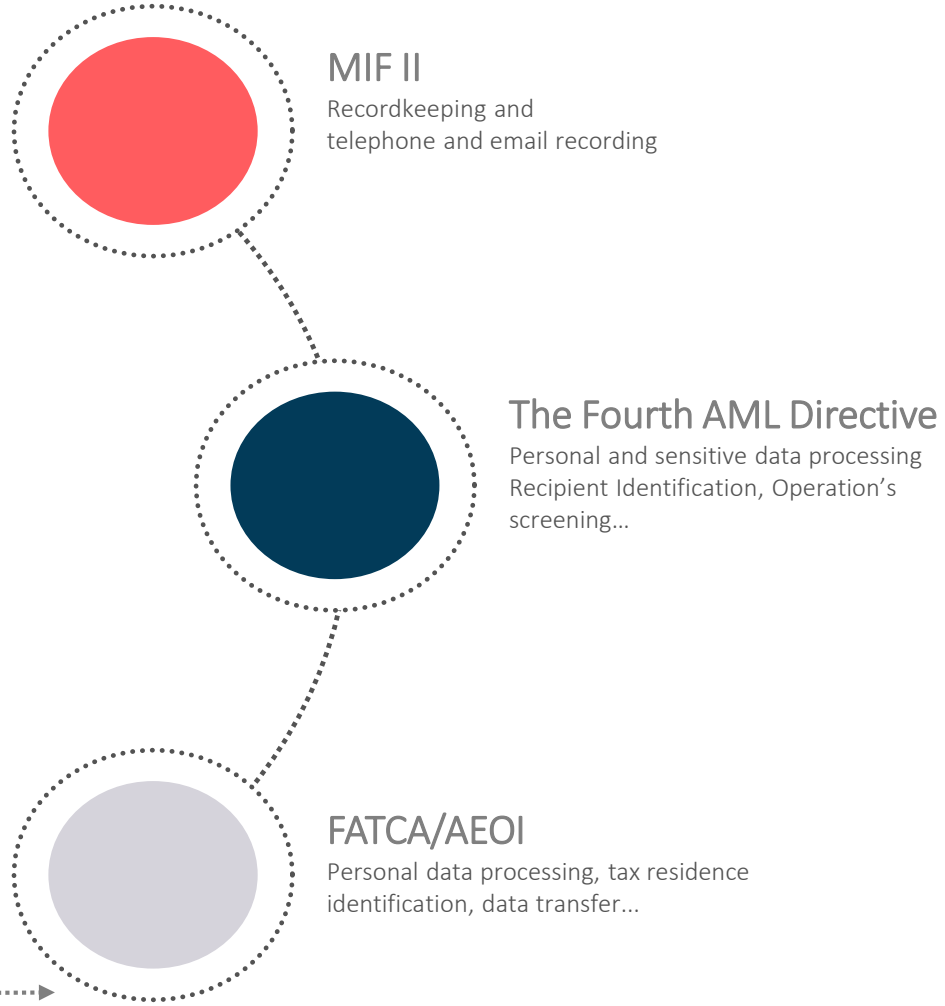
Regulatory framework

General Data Protection Regulation – Aurexia Consulting

GDPR

The entire regulatory framework, included Directives and Regulations, is highly demanding in terms of collect, storage and processing of personal data.

In order to bring a Data aware culture and to put your data processing as your key asset, we propose you to coordinate these regulatory projects to optimize the identification of the required resources to take advantage of the « putting together » opportunities related to these regulatory requirements.



PSD 2 ····· PRIIPS ····· IDD

Aurexia CONSULTING

Scope

Application…
…to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data.

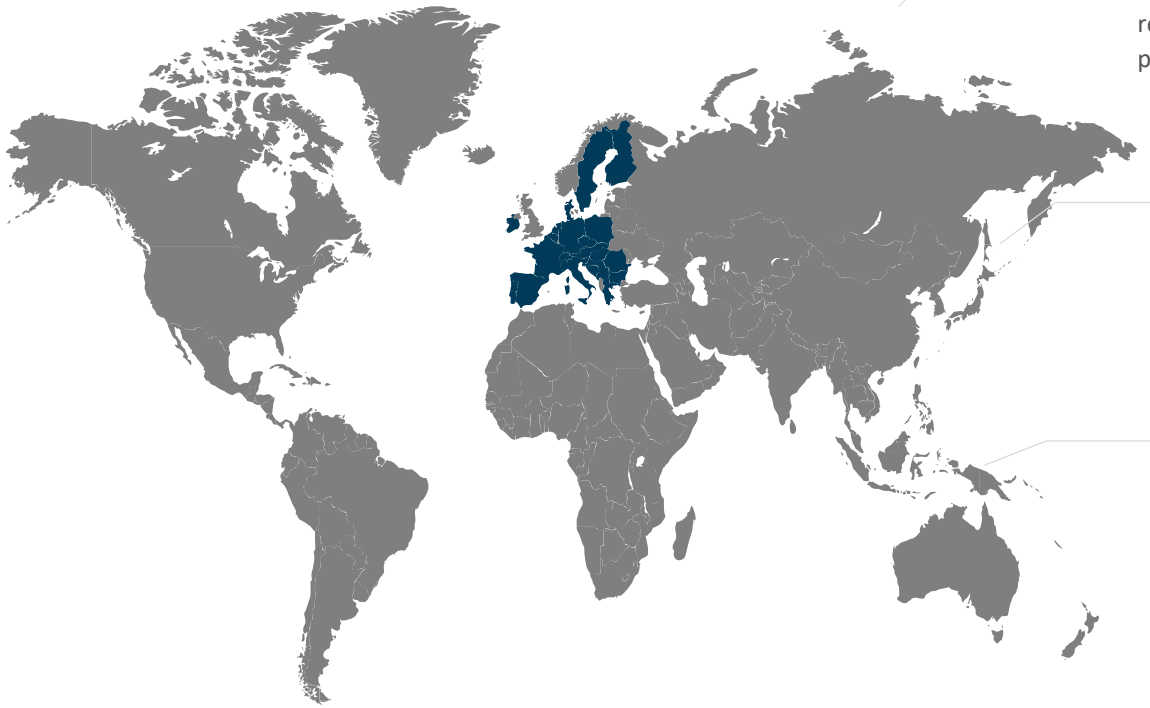
No application…
…to the processing of personal data…

…in the course of an activity which falls outside the scope of Union law;

…by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

…by a natural person in the course of a purely personal or household activity;

…by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.



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, Art 3 (1);

Processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, Art 3 (2);

Processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law, Art 3 (3).

Material scope

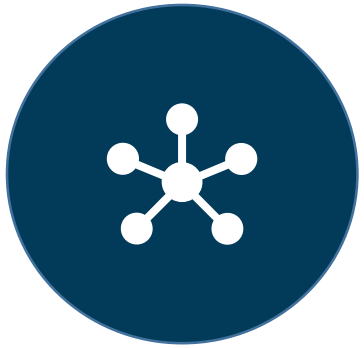
Territorial scope

Aurexia CONSULTING

Objectives of GDPR

Protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data

Protection of fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data



The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data

…Regulatory requirements which lead to new organizational goals…

Discover
(Identify personal data and where it resides)

Manage
(Govern how personal data is used and accessed)

Protect
(Establish security controls to prevent, detect and respond to Data breaches)

Report
(Address Data request, Breach notification, Records)

Aurexia CONSULTING

Turn GDPR objectives on a value added strategy

GDPR objectives	Reinforcement of data protection regulatory framework on Europe	Compliance requirements strengthen (Privacy by Design / Accountability)	Strict usage of data (Data minimization / Portability)	Client consent	Controls & Breach disclosure

Your approach to GDPR

Drive compliance by mastering your data management and protection to create added-value to your customers

Limit potential consequences

Regulation Penalties
Litigation
Reputation

Increase your Competitiveness

Aurexia CONSULTING

Aurexia's GDPR methodology

General Data Protection Regulation – Aurexia Consulting

GDPR assessment

The first step is to understand the GDPR impacts on your organization by:

- Establishing the landscape of personal information captured, stored and processed;
- Evaluate the current maturity of information governance, security controls an associated privacy processes throughout your organization;
- Evaluate the technical and operational maturity of your organization to meet the GDPR requirements and ensure a consistent methodology.

The GDPR assessment phase will vary according to the current level of compliance and data privacy awareness for your organization. Following this statement, an initial baseline of data privacy maturity will be determined and a Privacy Impact Assessments will be undertaken driven by the gap assessment and associated risk.

- **Regulation analysis (key changes)**
- **Impact assessment**
- **Gap assessment (Dpt by Dpt + workshops)**
- **Develop internal awareness and understanding**

GDPR roadmap

As a view of the landscape of personal information and the current level of compliance maturity are established , an action plan is undertaken to create an overall GDPR roadmap that:

- Identifies a set of tasks that your organization needs to execute to meet the compliance deadline;
- Provides a view of all dependencies of the identified tasks through your GDPR implementation project;
- Evaluates the resource allocation and cost estimates;
- Establishes a governance and RACI matrix

- **Governance set up**
- **Work streams identification**
- **Time frame identification (prioritization)**
- **Action plan (Work Breakdown Structure)**

GDPR Implementation

Driven from the findings of the GDPR assessment and the GDPR roadmap, the implementation phase will covered the following elements:

- Updates of policies – i.e data privacy policies, data protection officer role, accountabilities;
- Definition/updates of key processes to support requests under individual rights (subject access request, erasure requests etc), embedding of privacy by design into existing processes as well as data protection impact assessments into system/process development methodologies;
- IT solutions – Aurexia can help to identify your internal IT capabilities and/or to find an external solution with IT providers for the security of the information (data encryption…), data management (data quality, anonymization, reports…) and innovative solution (breach notification…)
- Support the change management (trainings…)

- **Personal Data processing identification**
- **Data protection Impact Assessment**
- **Policies and processes updates/creation**
- **Recordkeeping requirements (audit trail)**

Aurexia CONSULTING

Why Aurexia Consulting ?

OUR PEOPLE	OUR CULTURE	OUR ENGAGEMENTS	OUR LEADERSHIP
What makes Aurexia special is a unique blend of industry expertise, a solution oriented mind-set and best in class transformation skills. Aurexia consultants are decisive in scoping, launching and implementing their clients' projects.	We support and encourage an entrepreneurial outlook and independent thinking. Aurexia is not about hierarchy and organizational charts, we believe in a flat structure empowering all employees to feel that this is their firm to own and run.	Regulatory Engagements: Analyzed, designed and implemented regulator changes; Operational Transformation: drived operational efficiency projects, by designing, implementing and managing remedial changes.	From our research we have developed several points of view on the topic of privacy and data protection with resources trained and knowledgeable in privacy. With a strong project management approach and with experiences in regulatory topics implementation, our team members can deliver a full service from the assessment to the implementation that will drive compliance.

Contact us about how Aurexia Consulting can help you to make a step forward in your GDPR implementation

Aurexia CONSULTING

They trust us!

General Data Protection Regulation – Aurexia Consulting

Asset Management

BNP PARIBAS ASSET MANAGEMENT

AXA INVESTMENT MANAGERS

Amundi ASSET MANAGEMENT

ROTHSCHILD

NATIXIS ASSET MANAGEMENT

European Capital Partners

FEDERAL FINANCE

LA BANQUE POSTALE ASSET MANAGEMENT

Securities – Funds - Asset Services

BNP PARIBAS SECURITIES SERVICES

caceis INVESTOR SERVICES

Standard Chartered

FUNDROCK management company

European Fund Services

SOCIETE GENERALE Securities Services

PRO CAPITAL

VEGA INVESTMENT MANAGERS

Private Banking Retail Banking

SOCIETE GENERALE

Société Générale Bank & Trust

BGL BNP PARIBAS

SOCIETE GENERALE Private Banking

BANQUE PRIVÉE 1818

BanqueAccord

Allianz Banque

CréditMutuelArkéa

ING DIRECT Créateur d'intérêt

CAISSE D'EPARGNE

BNP PARIBAS WEALTH MANAGEMENT

GROUPE BPCE

Corporate Banking

SOCIETE GENERALE Corporate & Investment Banking

BNP PARIBAS CORPORATE & INVESTMENT BANKING

Santander

CRÉDIT AGRICOLE CORPORATE & INVESTMENT BANK

NATIXIS

HSBC

DEXIA

Caisse des Dépôts

Insurance

AG2R LA MONDIALE

CRÉDIT AGRICOLE ASSURANCES

NATIXIS ASSURANCES

Groupama

BPCE ASSURANCES

MUTAVIE

MACIF

Aurexia CONSULTING

Our Worldwide locations

PARTNER

Dominique HERROU

PARTNER

Éric VERNHES

PARTNER

David VILLARD

PARTNER

Charles BAIN de la COQUERIE

COO

Caroline SMADJA

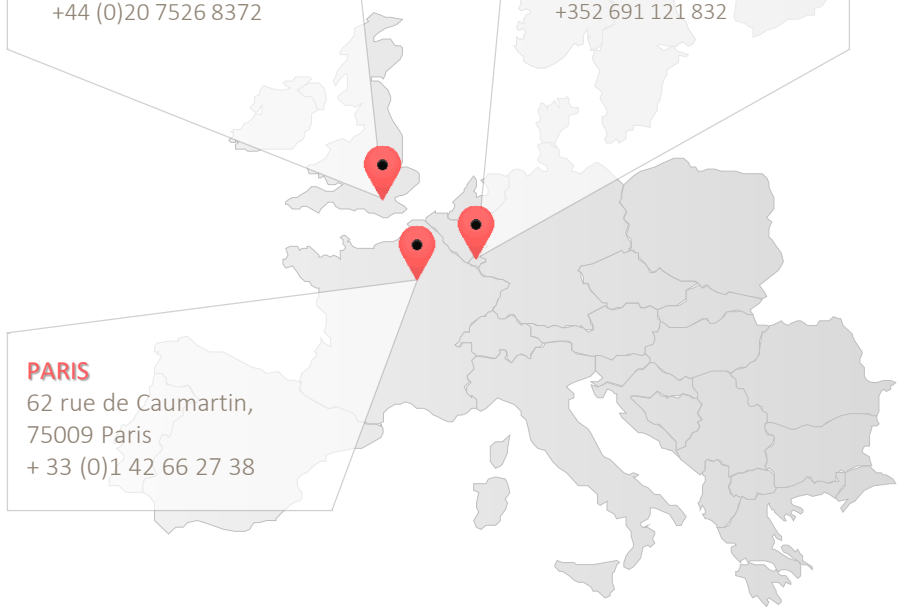
EUROPE

Swann REDSLOB

LONDON
1 Fore Street
London EC2Y 5EJ
+44 (0)20 7526 8372

Alain de CIDRAC

LUXEMBOURG
9 rue Large
L-1917 Luxembourg
+352 691 121 832



PARIS
62 rue de Caumartin,
75009 Paris
+ 33 (0)1 42 66 27 38

ASIA

Ludovic DUFETEL

HONG KONG
135 Bonham Strand
Sheun Wan, Hong Kong

Dominique HERROU

SINGAPORE
96 Robinson Road
#11-04 SIF Building
Singapore 068899
+ 65 9786 3870

Aurexia CONSULTING