GDPR and Fifth Step's "Virtual" Data Protection Officer

What is the General Data Protection Regulation (GDPR)?

The General Data Protection Regulation (GDPR) is the European Union's data protection regulation coming into force in 2018. It will affect all organisations holding or processing data pertaining to EU citizens. GDPR replaces the European Data Protection Directive (DPD) that came into force in December 1995. In serious cases of non-compliance, fines up to 20 million Euros, or 4% global turnover, whichever is the greater can be levied against the offending organisation.

How is GDPR different from DPD

1. New regulatory powers for the Information Commissioners Office (ICO), including audit, orders to cease business, suspension of data processing or operations to third countries
2. Companies processing sensitive data must appoint a Data Protection Officer (DPO)
3. Requirement to conduct Privacy Impact Assessments (PIA) against any processing involving sensitive personal data
4. Businesses must show greater accountability for the validation, protection and destruction of personal data
5. The business must be able to demonstrate documented policies and procedures in line with GDPR
6. The client retains ownership of the data they have supplied and may be entitled to request the raw telematics data for portability
7. Failure to comply may result in penalties; specifically, strict fines may be imposed, for serious breaches

The GDPR organisation

One of the significant points with GDPR is that it clearly defines the organisational roles involved in the activities of processing personal data:

- **Data Subject:** The individual who is the subject of the personal data
- **Data Controller:** The person who determines the manner in which the data will be processed -
- **Data Processor:** The person or organisation that processes the data
- **Data Protection Officer:** The person responsible for ensuring compliance, risk reduction and control of the data on behalf of the business. A nominated Data Protection Officer is a mandatory role to be compliant with GDPR.

> "In serious cases of non-compliance, fines up to 20 million Euros, or 4% global turnover, whichever is the greater can be levied against the offending organisation."

+44 (0)20 7193 1966 enquires@fifthstep.com www.fifthstep.com

The Purpose of the Data Protection Officer (DPO)

Companies processing sensitive data (client's personal data), and that fall within EU conditions of GDPR must appoint a Data Protection Officer (DPO), that is an individual expressly responsible for the task.

Tasks of the data protection officer

The data protection officer provides the expertise and knowledge to ensure the organisation adheres to GDPR, where relevant acts as the catalyst for actions and defines activities that require specialist knowledge. The DPO is likely an institutional expert with understanding of Information Security practices (although not stated as mandatory).

The Data Protection Officer shall be responsible for the following:

1. Ensure those who process or use personal data are aware of their responsibilities
2. Ensure the assignment of responsibility, awareness and training of staff
3. To advise and ensure that GDPR regulation is adhered to and advise on remediation in instances of non-compliance
4. To act as the intermediary and cooperate with the supervisory body
5. Advise on the processing operations, taking into account the nature, scope, context and purposes of processing
6. Act as point of contact in the event of a security breach

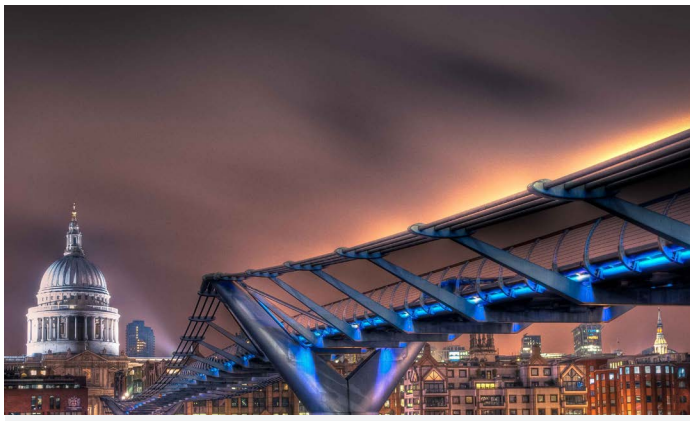
Importance of the DPO

Beyond the core requirement to meet GDPR compliance the DPO is there to endure the organisation constantly test and improve its data processing practices. The DPO provides clear guidance on importance of policies and procedures, constantly review and drive improvements.

Reality of GDPR and the DPO

Brexit is unlikely to reduce the impact of GDPR on UK businesses; the regulation comes into force before the UK plans to leave the EU. It is also likely that GDPR will be adopted for the foreseeable future because the UK government has made clear indication that they will carry over laws and regulation that are fit for purpose. It is also recognised that GDPR is a positive improvement to current standards as proved by the New York Department of Financial Services recent publication that it too intends to publish a GDPR like standard, and enforce in 2018.

The improvements in data protection that GDPR brings and he greater commitment globally to protecting personal data, it is probably that a DPO like role is fixed in the future landscape of businesses. The reality is that most small to medium organisations do not have the bandwidth or need for a full time resource.



"Brexit is unlikely to reduce the impact of GDPR on UK businesses; the regulation comes into force before the UK plans to leave the EU"

Fifth Step's Virtual Data Protection Officer (VDPO)

Fifth Step's VDPO service delivers expertise when and where you need it, to manage the transition to a GDPR compliant environment, whilst leveraging the organisations existing workforce. Providing support and guidance to those who use and manage personal information specifically. Our consultants are experts in Data Protection principles and developing the practices to achieve GDPR compliance, and maintain that status through constant review and improvement.

The Fifth Step VDPO service

Fifth Step is not new to the "virtual" solution provision model. We have run Virtual Security Officers, and Virtual Chief Information Security Officer services for years. It is a model that works, is efficient and cost effective for our clients. Dependent on the complexity and size of the organisation we can commit our SME's for one to many working days a month. This commitment is totally flexible so that it can "flexed up, or flexed down" without any penalties or blind cost. You pay for what is used. We will of course give clear guidance on what is the right commitment.

+44 (0)20 7193 1966 enquires@fifthstep.com www.fifthstep.com

GDPR and Fifth Step's "Virtual" Data Protection Officer

The Fifth Step approach

The VDPO provides an end-to-end solution, applying regulations expertise on a flexible basis. Committing our experts when, and where they are needed. Additional benefits of using our VDPO are they are all ISO27001 SME's, understand the Insurance industry and have exposure to ISO22301. This alone provides a level of understanding that provides total understanding of security data, systems and personnel.

End-to-end solution

Fifth step takes a service-based approach to the transformation/transform process to a compliant GDPR environment. This means we work with your team, leverage solid PM practices to create streams of work where needed, and focus on the smooth running of the data processing environment.

Our approach is structured and modular, committing to those areas where needed most, with our end-to-end approach is as follows:

1. Asses:
   a. Conduct current state assessment and identify gap analysis against GDPR
   b. Initiate simple remediation's
2. Plan:
   a. Develop a plan of change
   b. Agree ownership and communicate responsibilities
3. Deploy
   a. Support any physical change
   b. Manage any policy and process remediation
   c. Complete operational change & awareness program
   d. Conduct training and awareness
   e. Complete all work streams
4. Operate
   a. Monthly operational review
   b. Ad-Hoc compliance response
   c. Training and awareness
   d. Ongoing compliance review
   e. Act as the first point of contact

Key activities of the VDPO

We adhere closely to the GDPR standards and recommendations but sprinkle the magic that comes from having years of experience. Fifth Step identifies the following as a key activity list:

1. Ensure that decision makers in the organisation are aware of the changing law
2. Make sure that all the personal data you hold is documented, its source and origination
3. Review current privacy notices and plan changes
4. Review data processes and procedure, particularly how consent is sought and recorded
5. Verify data processing processes and document
6. Verify age of individuals and gather parental or guardian approval, ensuring all records are updated
7. Update policies
8. Identify a Data Protection Officer

"Fifth Step's working model is very simple. We practice flexible working, we do not advocate land and expand like the big 5 consultancies"

Benefits of the Fifth Step VDPO

- Our Data Protection Officers are industry and compliance experts, committed to Data Protection, Information Security and Business Continuity practices
- Fifth Step's working model is very simple. We practice flexible working, we do not advocate land and expand like the big 5 consultancies
- We are service orientated, that is we believe in long term relationships, and the way to make them work is deliver on our promise of continual improvement
- Our flexible working practices is supported by our commitment to our staff. We only use permanent members of staff of associates we have had a long working relationship with
- We established our organisation on the flexible model and control our costs through running a smart, not lean. We are therefore able to keep costs low and pass that benefit to our client. Which means we have great client retention, and are uniquely successful in winning new clients

For further information regarding Fifth Step's VDPO service please contact:

Wayne Jolly
Head of Security
e: wayne.jolly@fifthstep.com
p: 07939 151354