MSPWorld
POWERED BY MSPAlliance®

Robert J. Scott

GDPR: What Every MSP Needs to Know

Speaker

Robert J. Scott

#MSPWorld #MSPAlliance

MSPWorld
POWERED BY MSPAlliance®

Agenda

- Purpose
  - GDPR Intent & Obligations
- Applicability
  - Subject-matter and objectives
  - Material scope
  - Territorial scope
- New Rights
  - Right to rectification
  - Right to be Forgotten
  - Right to restriction of processing
  - Right to Data Portability
  - Right to Object
  - Privacy by Design
  - Privacy by Default
  - Consent
- Enforcement – Why you should care?
  - Supervisory Authority
  - Data Protection Authority
  - European Data Protection Board
  - Fines
  - Private Right of Action
- Roadmap / Decision Tree
  - Territorial Scope
  - Types of "personal data" in possession
  - Types of entities under GDPR – Controller / Processor / Sub-processor
  - Use Case Analysis - Processor
    - Chart Analysis
  - Legal requirements for compliance – processors and sub-processors
- Expert Advice
  - Preparing for GDPR
    - Contract Compliance
    - Processing Compliance

MSPWorld POWERED BY MSPAlliance

#MSPWorld #MSPAlliance

Purpose – Intent & Obligations

- The European General Data Protection Regulation ("GDPR") states that the processing of personal data is a fundamental right, which needs protection.

- GDPR imposes specific obligations on "Processors", "Controllers", and others with regard to their vendor relationships and the protection of "Personal Data".

- GDPR requires companies to conduct appropriate due diligence on processors and to have contracts containing specific provisions relating to data protection.

Applicability

Subject-Matter and Objectives of GDPR:

- The Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. (Art. 1(1))

- The Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. (Art. 1(2))

- 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. (Art. 1(3))

Applicability

Material Scope - So, GDPR applies when:

- Personal data is processed in connection with the goods or services to EU citizens, irrespective of payment. (Art. 3(2)(a))
- EU data subjects' behavior is monitored. (Art. 3(2)(b))

Territorial Scope - So, who does GDPR apply to?

- **EU Organizations** – GDRP applies to organizations that are established in the EU. (Art. 3(1))
- **Non-EU Organizations** – GDPR applies to organizations that process Personal Data about people in the EU. (Art. 3(1))
  - GDPR is an extraterritorial law, meaning it may affect US companies and MSPs. If an MSP processes Personal Data about EU people, the law will affect the MSPs business operations. Processing must be done in accordance with GDPR guidelines.

- **International Data Transfers**: If an MSP transfers data outside the EU or EEA, then the MSP must be complaint with GDPRs guidelines.

New Rights

- **Right to rectification** - data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. (Art. 16)
- **Right to be Forgotten** - Explicit right to be forgotten – personal data must be erased “without undue delay” when:
    - Retention is not required.
    - Data is no longer needed.
    - Consent is withdrawn.
- May have a significant impact on how controllers and processors do business. (Art. 17)
- **Right to restriction of processing** – Data subject has the right to obtain from the controller restriction of processing where: (Art. 18)
    - Accuracy of data is contested
    - Processing is unlawful
    - Controller no longer needs the personal data for the purposes of processing
    - Data subject has objected to processing pursuant Art 21(1) – Right to Object.
- **Right to Data Portability** - When data is processed by automated means (i.e. a cloud service provider) individuals have the right to transmit the data to another service provider when it is technically feasible. (Art. 20)
- **Right to Object** - data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. (Art. 21)

New Rights

- **Privacy by Design** – Emphasis on adopting appropriate policies and safeguards to protect personal data.
  - Companies must draft, adopt, and implement appropriate technical, physical, and administrative measures to protect personal data prior to, and continually monitor during, processing of personal data during the whole life cycle of the system or process development.
  - The draft text of the GDPR uses the term transparency a number of times – a company must be clear and transparent in their dealings with individuals. (Art. 25)

- **Privacy by Design** – Data Controllers will no longer need to submit routine notifications to a Data Protection Authority ("DPA").
  - Instead, controllers and processors will need to keep detailed internal records of personal data processing.
  - Includes named/contact information for data processors, controllers, and joint controllers. (Art. 30)

  - **Exemption from documentation requirements:** Small and Medium Enterprises (SME) with less than 250 employees will not need to comply with this unless their activities meet certain requirements deemed to be risky to privacy. (Art. 30(5))

- **Privacy by Default** - Privacy by Default simply means that the strictest privacy settings automatically apply once a customer acquires a new product or service. In other words, no manual change to the privacy settings should be required on the part of the user. There is also a temporal element to this principle, as personal information must by default only be kept for the amount of time necessary to provide the product or service. (Art. 25)

New Rights

- **Consent** – Discussed earlier regarding processing of personal data. However, consent must be given by clear affirmative action in order to establish a freely given, specific, informed, and unambiguous agreement to the processing. The following are a few points to remember:
  - Consent is not freely given if "clear imbalance between data subject and controller, particularly when controller is a public authority." (Recital #43)
  - Controller cannot make service conditional upon consent unless processing is necessary for service. (Art. 7(4))
  - Specific to data collection purpose. New consent for additional processing that is *incompatible* with the original purpose. (Art. 5(1)(b) & Art. 7(1))
  - Affirmative, opt-in consent (not opt-out). Can be shown by a statement or conduct with clearly indicates acceptance. (Art. 7(2))
  - Consent can be withdrawn at any time – controllers must inform data subjects of the right to withdraw before consent is given. (Art. 7(3))
  - Verifiable, parental consent required for collection of personal data of a minor
    - Each state can determine age of consent 13 or above (generally 16). (Art. 8(1))
  - Explicit consent required for processing of the special categories of personal data. (Art. 9)
    - This includes "Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited," unless consent is given. (Art. 9(1))

Enforcement – Why you should care?

- **Supervisory Authority (“SA”)**– is an independent public authority from each Member State in the EU with the authority to regulate compliance with GDPR.
- **Data Protection Authority** - is an independent public authority responsible for monitoring the application of data protection law within its territory.
- **European Data Protection Board (“EDPB”)** - The old Article 29 “Working Party” will become the European Data Protection Board. The EDPB has the status of an EU body with legal personality and extensive powers to determine disputes between national supervisory authorities, to give advice and guidance and to approve EU-wide codes and certification.

Enforcement – Why you should care?

- **Fines** – Supervisor Authorities may impose monetary fines on data controllers and processors for violations. Two different levels:
  - Up to 10M EUR or 2% of organization's prior year's worldwide turnover. (Art. 83(4))
  - Up to 20M EUR or 4% of organization's prior year's worldwide turnover. (Art. 83(5))

- **Private Right of Action** - GDPR maintains the private right of action for damages.
  - But now extended to actions against data processors for breaches of the applicable sections of GDPR.
  - Burden of proof lies with the data controller and/or processor. (Art. 79, Art. 82)

Roadmap & Decision Tree

- The following steps should be followed to ascertain whether a business is required to be compliant with GDPR, and what steps need to be taken to prepare:
  - Territorial Scope
    1. Is your business located in the EU? (Art. 3(1))
       - Yes, go to question #4 to determine what "personal data" is in your possession.
       - No, go to question #2.
    2. Are you offering goods or services in EU, regardless of whether payment is required? (Art. 3(2)(a))
       - Yes, go to question #4 to determine what "personal data" is in your possession.
       - No, go to question #3.
    3. Are you monitoring the behavior of EU data subjects, as far as their behavior takes place in the EU? (Art. 3(2)(b))
       - Yes, go to question #4 to determine what "personal data" is in your possession.
       - No, go to question #4 to determine what "personal data" is in your possession.

Roadmap & Decision Tree

- Types of “personal data” in possession

4. Is the “personal data” you have in your possession any of the following: any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person?* (Art. 4(1))

* For some organizations, the explicit inclusion of **location data**, **online identifiers** and **genetic data** within the definition of "personal data" may result in additional compliance obligations (e.g., for online advertising businesses, many types of cookies become personal data under the GDPR, because those cookies constitute "online identifiers").

- Yes, go to question #5.
- No, go to question #5, to determine if you are “processing” personal data of EU data subjects.
  - If you do not have any personal data of an EU data subject in your possession, then you are not subject to GDPR.
  - If you are not: (1) located in the EU, and (2) you are not offering goods or services in the EU, and (3) you are not monitoring behavior of EU data subjects, then you are not subject to GDPR

MSPWorld POWERED BY MSPAlliance

#MSPWorld #MSPAlliance

Roadmap & Decision Tree

- Types of “personal data” in possession

5. Are you “processing” personal data of EU data subjects? (Art. 4(2))

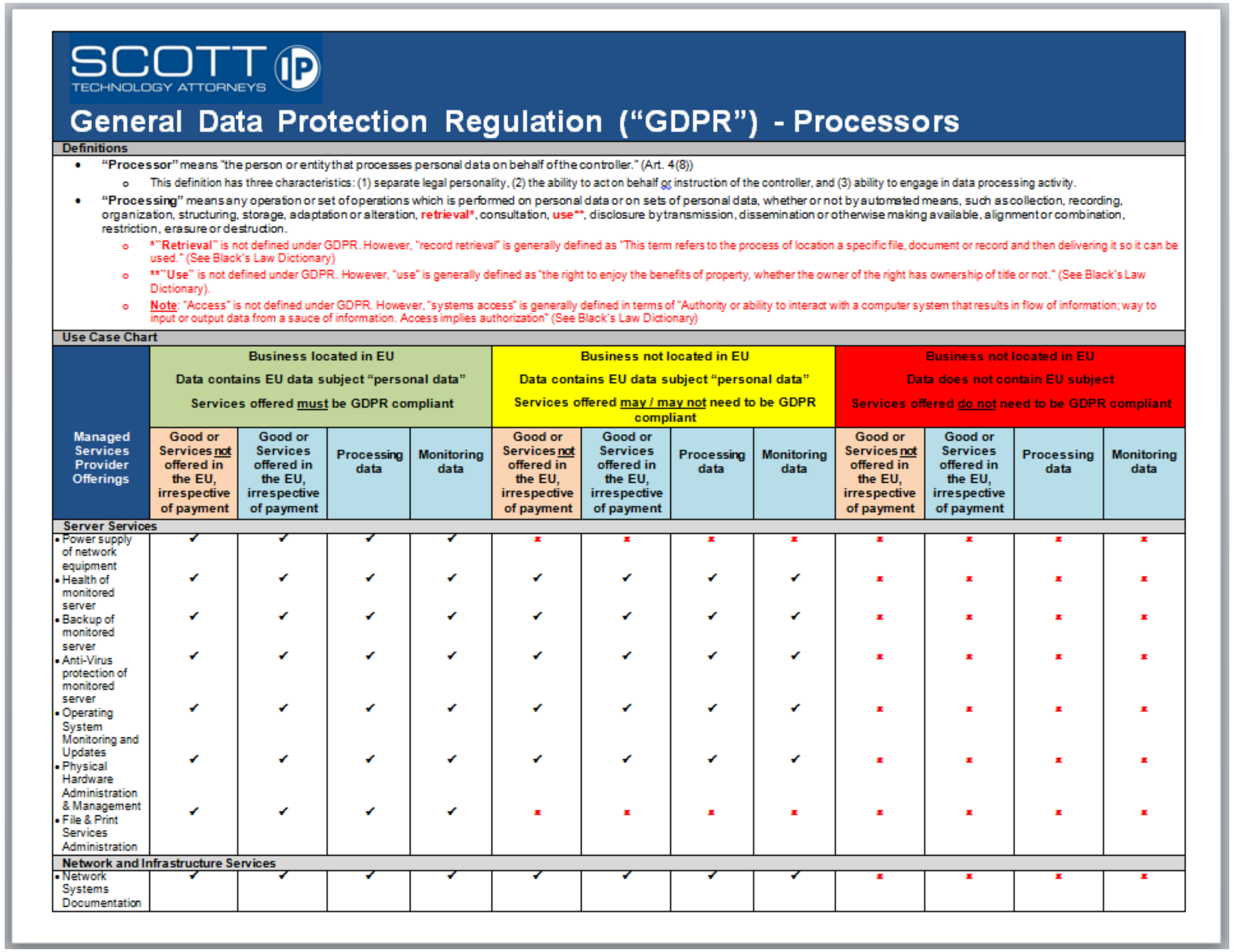
*”Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, **use**, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

**Please see our Use Case chart for further examples of activities that are considered “processing” before answering this question.

- Yes, go to question #6.
- No.
  - If you are not processing personal data of an EU data subject, then you are not regulated under GDPR. However, if you “**use**” personal data of an EU data subject in anyway then you may be regulated under GDPR.

Roadmap & Decision Tree

Use Case Chart – Service Offerings



SCOTT IP
TECHNOLOGY ATTORNEYS

General Data Protection Regulation (“GDPR”) - Processors

Definitions

- **“Processor”** means “the person or entity that processes personal data on behalf of the controller.” (Art. 4(8))
  - This definition has three characteristics: (1) separate legal personality, (2) the ability to act on behalf or instruction of the controller, and (3) ability to engage in data processing activity.
- **“Processing”** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, **retrieval***, consultation, **use****, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
  - *“**Retrieval**” is not defined under GDPR. However, “record retrieval” is generally defined as “This term refers to the process of location a specific file, document or record and then delivering it so it can be used.” (See Black’s Law Dictionary)
  - **“**Use**” is not defined under GDPR. However, “use” is generally defined as “the right to enjoy the benefits of property, whether the owner of the right has ownership of title or not.” (See Black’s Law Dictionary).
  - Note: “Access” is not defined under GDPR. However, “systems access” is generally defined in terms of “Authority or ability to interact with a computer system that results in flow of information; way to input or output data from a sauce of information. Access implies authorization” (See Black’s Law Dictionary)

Use Case Chart

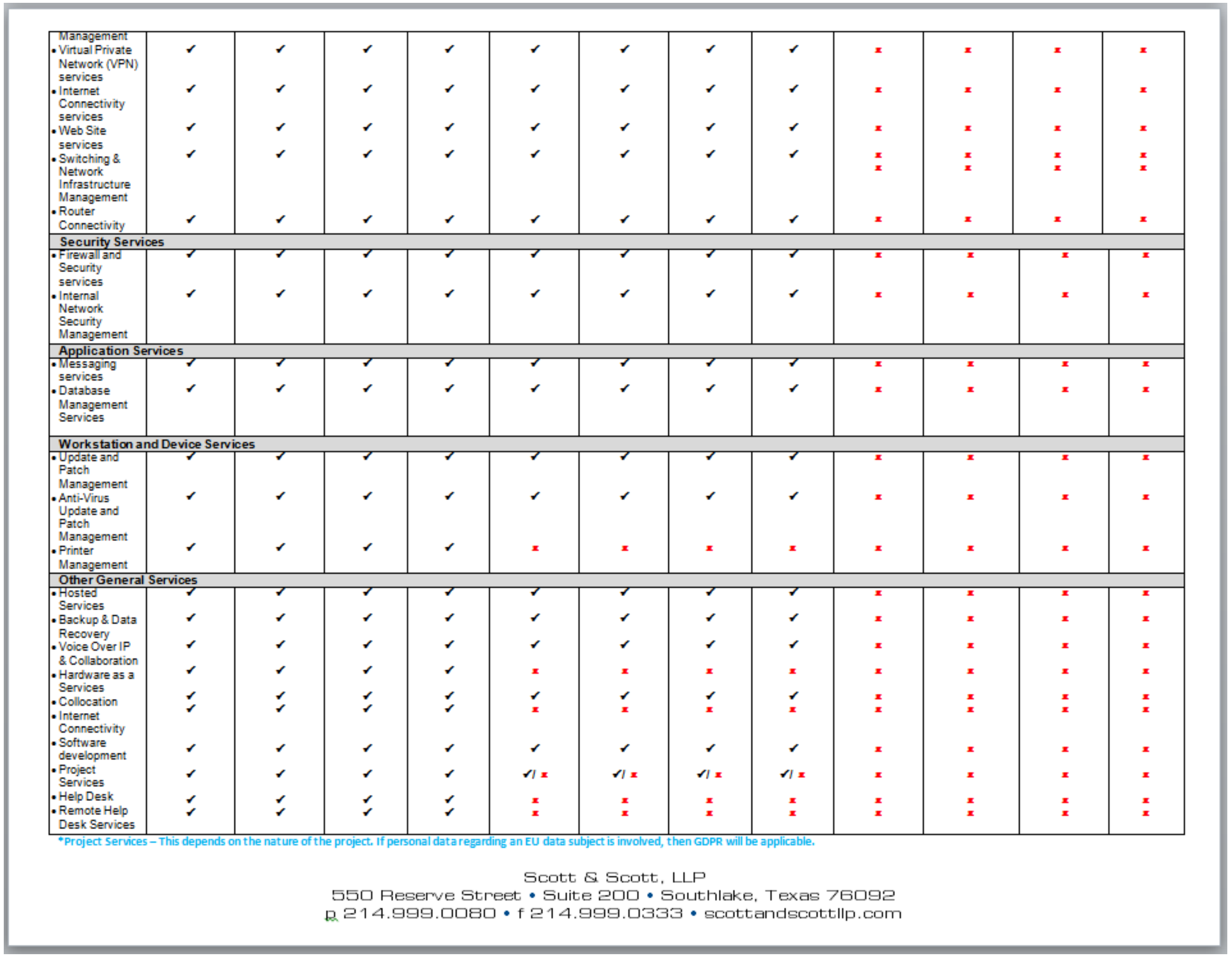
Managed Services Provider Offerings	Business located in EU Data contains EU data subject “personal data” Services offered must be GDPR compliant				Business not located in EU Data contains EU data subject “personal data” Services offered may / may not need to be GDPR compliant				Business not located in EU Data does not contain EU subject Services offered do not need to be GDPR compliant			
	Good or Services not offered in the EU, irrespective of payment	Good or Services offered in the EU, irrespective of payment	Processing data	Monitoring data	Good or Services not offered in the EU, irrespective of payment	Good or Services offered in the EU, irrespective of payment	Processing data	Monitoring data	Good or Services not offered in the EU, irrespective of payment	Good or Services offered in the EU, irrespective of payment	Processing data	Monitoring data
Server Services												
• Power supply of network equipment	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗
• Health of monitored server	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗
• Backup of monitored server	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗
• Anti-Virus protection of monitored server	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗
• Operating System Monitoring and Updates	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗
• Physical Hardware Administration & Management	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗
• File & Print Services Administration	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗
Network and Infrastructure Services												
• Network Systems Documentation	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗

MSPWorld
POWERED BY MSPAlliance

#MSPWorld #MSPAlliance

Roadmap & Decision Tree

Use Case Chart – Service Offerings



Management												
• Virtual Private Network (VPN) services	✓	✓	✓	✓	✓	✓	✓	✓	✘	✘	✘	✘
• Internet Connectivity services	✓	✓	✓	✓	✓	✓	✓	✓	✘	✘	✘	✘
• Web Site services	✓	✓	✓	✓	✓	✓	✓	✓	✘	✘	✘	✘
• Switching & Network Infrastructure Management	✓	✓	✓	✓	✓	✓	✓	✓	✘ ✘	✘ ✘	✘ ✘	✘ ✘
• Router Connectivity	✓	✓	✓	✓	✓	✓	✓	✓	✘	✘	✘	✘
Security Services												
• Firewall and Security services	✓	✓	✓	✓	✓	✓	✓	✓	✘	✘	✘	✘
• Internal Network Security Management	✓	✓	✓	✓	✓	✓	✓	✓	✘	✘	✘	✘
Application Services												
• Messaging services	✓	✓	✓	✓	✓	✓	✓	✓	✘	✘	✘	✘
• Database Management Services	✓	✓	✓	✓	✓	✓	✓	✓	✘	✘	✘	✘
Workstation and Device Services												
• Update and Patch Management	✓	✓	✓	✓	✓	✓	✓	✓	✘	✘	✘	✘
• Anti-Virus Update and Patch Management	✓	✓	✓	✓	✓	✓	✓	✓	✘	✘	✘	✘
• Printer Management	✓	✓	✓	✓	✘	✘	✘	✘	✘	✘	✘	✘
Other General Services												
• Hosted Services	✓	✓	✓	✓	✓	✓	✓	✓	✘	✘	✘	✘
• Backup & Data Recovery	✓	✓	✓	✓	✓	✓	✓	✓	✘	✘	✘	✘
• Voice Over IP & Collaboration	✓	✓	✓	✓	✓	✓	✓	✓	✘	✘	✘	✘
• Hardware as a Services	✓	✓	✓	✓	✘	✘	✘	✘	✘	✘	✘	✘
• Collocation	✓	✓	✓	✓	✓	✓	✓	✓	✘	✘	✘	✘
• Internet Connectivity	✓	✓	✓	✓	✘	✘	✘	✘	✘	✘	✘	✘
• Software development	✓	✓	✓	✓	✓	✓	✓	✓	✘	✘	✘	✘
• Project Services	✓	✓	✓	✓	✓/ ✘	✓/ ✘	✓/ ✘	✓/ ✘	✘	✘	✘	✘
• Help Desk	✓	✓	✓	✓	✘	✘	✘	✘	✘	✘	✘	✘
• Remote Help Desk Services	✓	✓	✓	✓	✘	✘	✘	✘	✘	✘	✘	✘

*Project Services – This depends on the nature of the project. If personal data regarding an EU data subject is involved, then GDPR will be applicable.

Scott & Scott, LLP
550 Reserve Street • Suite 200 • Southlake, Texas 76092
p 214.999.0080 • f 214.999.0333 • scottandscottllp.com

MSPWorld
POWERED BY MSPAlliance®

#MSPWorld #MSPAlliance

Roadmap & Decision Tree

- Types of entities under GDPR – Controller / Processor / Sub-processor

6. Are you a "controller", "processor", or "sub-processor" of personal data regarding EU data subjects?? (Art. 4(2))

*"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

"Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

"Sub-processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the processor with controller's consent;

- Yes, go to question #7, 8, or 9.
- No.
  - If you are not processing personal data of an EU data subject, then you are not regulated under GDPR.

Roadmap & Decision Tree

- Legal requirements for compliance with GDPR – Controller / Processor / Sub-Processor

8. If you are a "Processor":

- You must meet the following to prepare for GDPR compliance:
  - **Contract/Transactional Compliance**
    - **Contract Updates & GDPR Addendum** – Include contract language to be in compliance with Processing or Controlling (Art. 28(6), Art. 46(3)(a))
    - **Security Policies** - Review, revise (or draft) your written information security policies to ensure appropriate technical, administrative, and physical measures are in place to protect data or to transfer data. (Art. 6, Art. 8, Art. 9, Art. 10, Art. 13, Art. 14)
    - **Privacy Policies** - Review and revise your privacy policies to ensure they are written in clear and plain language and fully disclose your data collection and processing practices. (Art. 6, Art. 8, Art. 9, Art. 10, Art. 13, Art. 14)
    - **Consent** - Review and update your method to obtain consent to ensure you get specific, informed, and unambiguous opt-in consent. (Art. 7 & 8)
    - **Appoint a Data Protection Officer ("DPO") or Consider Hiring One** – A Controller or Processor may need to appoint or hire a DPO to server on its behalf if local law requires it, or if data processing activities involve: systematic monitoring, or processing of sensitive personal data on a large scale. (Art. 37)
      - Hiring an attorney with expertise as a DPO creates attorney-client privilege, where the exchange of information is considered privileged and confidential.
    - **Non-disclosure Agreements / Confidentiality Agreements** – Must have a confidentiality agreement in place with employees. (Art. 28(3)(b), Art. 29)
    - **Insurance** - Review your insurance for scope and limits of coverage.

MSPWorld POWERED BY MSPAlliance

#MSPWorld #MSPAlliance

Roadmap & Decision Tree

- Legal requirements for compliance with GDPR – Controller / Processor / Sub-Processor

8. If you are a "Processor":

- You must meet the following to prepare for GDPR compliance:
  - **Processing Compliance**
    - Start a data inventory now. (Art. 29, 30, 33)
    - Put processes in place for Data Protection Impact Assessment (if needed). (Art. 35)
    - Maintain detailed records of personal data processing activities. (Art. 5, 6, 7, 8, 9, 10, 11, 30)
      - **Processing Compliance - Processing Principles - Personal data shall be processed**:
        - Lawfully, fairly, and transparently (Art. 5(1)(a))
        - **Purposely collected with limited scope** – "Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes…" (Art. 5(1)(b))
        - **Data minimization** – "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (Art. 5(1)(c))
        - **Accurately** – " accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay" (Art. 5(1)(d))
        - **Limited storage** – "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed" (Art. 5(1)(e))
        - **Integrity and Confidentiality** – "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures." (Art. 5(1)(f))
        - **Accountability and Compliance** – "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1." (Art. 5(2))

Roadmap & Decision Tree

- **Processing Compliance Continued**
  - **Lawfulness of processing**
    - Processing shall be lawful only if and to the extent that at least one of the following applies:
      - **Consent** – "the data subject has given consent to the processing of his or her personal data for one or more specific purposes" (Art. 6(1)(a))
      - **Necessary for Contracting** – "processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract" (Art. 6(1)(b))
      - **Compliance with legal obligations** – "processing is necessary for compliance with a legal obligation to which the controller is subject" (Art. 6(1)(c))
      - **Protect vital interests** – "processing is necessary in order to protect the vital interests of the data subject or of another natural person" (Art. 6(1)(d))
      - **Performance of public interest task** – "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller" (Art. 6(1)(e))
      - **Legitimate interest** – "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." (Art. 6(1)(f))
    - Member States may maintain or introduce more specific requirements to ensure lawful and fair processing and compliance regarding points (3) and (5) above. (Art. 6(2))
  - **Conditions for consent**
    - **Proof of Consent** - Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. (Art. 7(1))
    - **Written Declaration** - If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. (Art. 7(2))

Roadmap & Decision Tree

- **Processing Compliance Continued**
    - **Withdraw Consent at any time** - The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. (Art. 7(3))
    - **Assessing Consent Freely Given** - When assessing whether consent is freely given, utmost account shall be taken of whether, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. (Art. 7(4))
  - **Conditions applicable to child's consent**
    - **Parental Consent** – "…the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child." (Art. 8(1))
    - **Lower Age** – "Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years." (Art. 8(1))
    - **Reasonable Efforts** – "The controller shall make reasonable efforts to verify in such cases that consent is given or authorized by the holder of parental responsibility over the child, taking into consideration available technology." (Art. 8(2))
    - **Affect on contract formation** – "Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child." (Art. 8(3))
- Adopt a "Privacy by Design" design strategy for your products and services. (Art. 5, 6, 7, 8, 9, 10, 11, 25)
- **Compliance with the controller's instructions** - Processors (and any sub-processors) shall not process personal data, except in accordance with the instructions of the controller, or the requirements of EU law or the national laws of Member States. (Art. 29)
- **Conflicts between the controller's instructions and applicable (EU) law** - In the event that a processor believes that the controller's instructions conflict with the requirements of the GDPR or other EU or Member State laws, the processor must immediately inform the controller. (Art. 28(3)(h))

Roadmap & Decision Tree

- **Processing Compliance Continued**
  - **Failure to comply with the controller's instructions** - Where a processor, in breach of the GDPR, determines the purposes and means of any processing activity (i.e., if the processor makes its own decisions, rather than following the controller's instructions), that processor is treated as a controller in respect of that processing activity. (Art. 28(10))
  - **Appointment of sub-processors** - The processor must not appoint a sub-processor without the prior written consent of the controller. Where the controller agrees to the appointment of sub-processors, those sub-processors must be appointed on the same terms as are set out in the contract between the controller and the processor. (Art. 28(2), (4))
  - **Processor's obligation of confidentiality** - The processor must ensure that any personal data that it processes are kept confidential. The contract between the controller and the processor must require the processor to ensure that all persons authorized to process the personal data are under an appropriate obligation of confidentiality. (Art. 28(3)(b), Art. 29)
  - **Data Security** - Processors must implement appropriate technical and organizational security measures to protect personal data against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access. Depending on the nature of the processing, these may include:
    - encryption of the personal data by **Pseudonymisation**;
      - **GDPR encourages pseudonymisation**:
        - Personal data is partially anonymized.
        - Personal data is split into two databases – one using an anonymous "key" and the other database that contains the lookup of the identifying information with the key.
        - Databases are held separately.
        - Requirement to use technical and administrative measures to prevent re-identification
    - on-going reviews of security measures;
    - redundancy and back-up facilities; and
    - regular security testing. (Art. 32)
  - **Assessing the appropriate level of security** - account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed. (Art. 32(2))

MSPWorld POWERED BY MSPAlliance®

#MSPWorld #MSPAlliance

Roadmap & Decision Tree

- **Processing Compliance Continued**
  - **Additional Steps to Prevent Access** - The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law. (Art. 32(4))
  - **Reporting Data Breaches to Controller** - Processors must notify any data breach to the controller without undue delay. (Art. 33)
  - **Restrictions on Cross-Border Data Transfers** - Under the GDPR, the obligations regarding Cross-Border Data Transfers apply directly to processors. (Art. 44)
  - **Liability of Processors** - Data subjects can bring claims directly against processors. However, a processor is liable for the damage caused by its processing activities only where it has:
    - not complied with obligations under the GDPR that are specifically directed to processors; or
    - acted outside or contrary to lawful instructions of the controller. (Art. 82(1)-(2))
  - **Assist controller with customer rights requests – Such as right to rectification, right to be forgotten, right to restriction of processing, right to data portability, right to object, etc. (Art. 16, 17, 18, 20, 21)**
  - **Get Certified.** (Art. 42)

Roadmap & Decision Tree

- Legal requirements for compliance with GDPR – Controller / Processor / Sub-Processor

9. If you are a "Sub-processor":

- You must follow the above guidelines for "processors" but also, must enter a contractual relationship with the processor with the consent of the controller to process the data. (Art 28(2), Art 28(4))

MSPWorld POWERED BY MSPAlliance

Expert Advice

- **Preparing for GDPR**
  - GDPR enforcement will begin around May 25, 2018.
  - GDPR requires significant changes for organizations who monitor or process EU citizen's personal data.
  - Time is much shorter than it seems to get the above mentioned items implemented. If you have not done so already, seek legal counsel.

Expert Advice

- ## Recap - Preparing for GDPR
  - ### Contract/Transactional Compliance
    - **Contract Updates & GDPR Addendum** – Include contract language to be in compliance with Processing or Controlling (Art. 28(6), Art. 46(3)(a))
    - **Security Policies** - Review, revise (or draft) your written information security policies to ensure appropriate technical, administrative, and physical measures are in place to protect data or to transfer data. (Art. 6, Art. 8, Art. 9, Art. 10, Art. 13, Art. 14)
    - **Privacy Policies** - Review and revise your privacy policies to ensure they are written in clear and plain language and fully disclose your data collection and processing practices. (Art. 6, Art. 8, Art. 9, Art. 10, Art. 13, Art. 14)
    - **Consent** - Review and update your method to obtain consent to ensure you get specific, informed, and unambiguous opt-in consent. (Art. 7 & 8)
    - **Appoint a Data Protection Officer ("DPO") or Consider Hiring One** – A Controller or Processor may need to appoint or hire a DPO to server on its behalf if local law requires it, or if data processing activities involve: systematic monitoring, or processing of sensitive personal data on a large scale. (Art. 37)
      - Hiring an attorney with expertise as a DPO creates attorney-client privilege, where the exchange of information is considered privileged and confidential.
    - **Non-disclosure Agreements / Confidentiality Agreements** – Must have a confidentiality agreement in place with employees. (Art. 28(3)(b), Art. 29)
    - **Insurance** - Review your insurance for scope and limits of coverage.
  - ### Processing Compliance
    - Start a data inventory now. (Art. 29, 30, 33)
    - Put processes in place for Data Protection Impact Assessment (if needed). (Art. 35)
    - Maintain detailed records of personal data processing. (Art. 5, 6, 7, 8, 9, 10, 11)
    - Adopt a "Privacy by Design" design strategy for your products and services. (Art. 5, 6, 7, 8, 9, 10, 11)
    - **Data Security** - Processors must implement appropriate technical and organizational security measures to protect personal data against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access. Depending on the nature of the processing. (Art. 32)
    - **Assist controller with customer rights requests – Such as right to rectification, right to be forgotten, right to restriction of processing, right to data portability, right to object, etc. (Art. 16, 17, 18, 20, 21)**

    Get Certified. (Art. 42)

#MSPWorld #MSPAlliance

Questions?

MSPWorld
POWERED BY MSPAlliance

#MSPWorld #MSPAlliance

Contact Information

Robert J. Scott, Esq.

Managing Partner

rjscott@scottandscottllp.com

(214) 999-2902

Scott & Scott, LLP.
1256 Main Street, Suite 200
Southlake, TX 76092
www.scottandscottllp.com