THE GDPR AND DFIR
THE IMPACT OF THE EU GENERAL DATA PROTECTION REGULATION ON DIGITAL FORENSICS AND INCIDENT RESPONSE
Digital forensics and incident response is fundamentally about digital evidence, and some of that evidence will be data that is affected by the European Union General Data Protection Regulation.
If you are performing digital forensics and incident response in the European Union, or for an organisation that does business in the European Union, or a European Union business operating outside of the European Union, then the GDPR will be applicable to you.
RELEVANT DEFINITIONS

ARTICLE 4
PERSONAL DATA

Any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, by a name, an identification number, location data, an online identifier, or factors such as physical, physiological, genetic, mental, economic, cultural or social that may lead to identifying a person.
PROCESSING

Any operation which is performed on personal data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
CONTROLLER

Any natural or legal person, public authority, agency or other body which alone or jointly with others determined the purposes and means of the processing of personal data.
PROCESSOR

A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
When it relates to personal data, all DFIR processes and activities will fall under the definition of processing, and most practitioners will fall under the definition of processors.
PRINCIPLES RELATING TO PROCESSING OF PERSONAL DATA

• In essence it must be done lawfully, fairly and transparently
• It must be done in a manner limited to what is necessary in relation to the purpose that it was initially processed
• Accuracy must be maintained
• It must only be kept for as long as necessary, and it must be secured
• Compliance must be demonstrated by the controller.
LAWFULNESS OF PROCESSING

• Consent of the data subject
• Processing is necessary for the performance of a contract of which the data subject is party of
• Processing is necessary for compliance with a legal obligation to which the controller is subject
• Processing is necessary in order to protect the vital interests of the data subject or another natural person
• Processing is necessary for a task in the public interest or by exercising official authority
• Processing is necessary for the purposes of legitimate interests of the controller or third party.
CONDITIONS FOR CONSENT

• The controller must be able to prove consent
• Before consent is given, the data subject must be notified that they can withdraw consent
• If the consent is in writing, it must be clear, and no part may infringe on the GDPR
• The data subject can withdraw consent at any time, but this does not apply to anything processed while consent was active
• It determining if consent is given freely, issues such as contractual obligations or service conditions must be considered
National member states may issue legislation impacting on some of these Articles in specific instances relating to investigations, regulatory and legal processes.
PROCESSOR REQUIREMENTS
ARTICLE’S 28, 29, 30
PROCESSOR

• A controller can only use a processor that provides sufficient guarantees that they will comply with the Regulations and protect the rights of data subjects
• A processor shall not engage another processor without permission of the controller
• Processing by a processor must be governed by a contract between the controller and processor which sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data involved, and the obligations and rights of the controller
THE PROCESSOR CONTRACT

• Processing personal data may only be done on documented instructions, including taking account transferring data to a third country or international organisation
• The processor must be committed to confidentiality
• Take all measures to comply with Article 32
• Respect all conditions relating to engaging another processor
• Assist the controller in fulfilling their obligations in terms of Chapter III and Articles 32 to 36
• Delete or return the personal data if requested by the controller unless a law requires storage
• Make available to the controller everything necessary to demonstrate compliance
RECORDS OF PROCESSING ACTIVITIES

• The name and contact details of the processor(s) and the controller on behalf of who they are acting, and where relevant the data protection officer
• The categories of processing carried out on behalf of each controller
• Where applicable transfers of data to a third country or international organisation, and the documentation of suitable safeguards
• Where possible a general description of the technical and organisational security measures applied
To comply with these provisions DFIR practitioners will need to ensure that they have appropriate mandates in place, as well as appropriate policies and procedures (where appropriate)
SECURITY OF PROCESSING

• The pseudonymisation and encryption of personal data
• The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
• The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
• A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing
DFIR practitioners must practice good information security. We need to do what we say.
JASON JORDAAN
CFCE, CFE, MCSFS, PMIITPSA, GCFE, GCFA
MSc, MTech, BComHons, BSc, BTech
PRINCIPAL PARTNER
jason@dfirlabs.com
+27 83 556 7112
www.dfirlabs.com
@DFS_JasonJ