GDPR Compliance – New Approach & New Challenges

NIKOLINAKOS - LARDAS & PARTNERS

LAW FIRM

NIKOLINAKOS - LARDAS & PARTNERS

LAW FIRM

Data Protection, Privacy & Cybersecurity Practice

Ranked #1 in Greece

Leading Experts in Data Privacy & Cybersecurity

The LEGAL 500 EMEA LEADING INDIVIDUAL 2017

RANKED IN EUROPE CHAMBERS 2016 LEADING INDIVIDUAL

The LEGAL 500 EMEA TOP TIER 2017

RANKED IN EUROPE CHAMBERS 2016 LEADING FIRM

NIKOLINAKOS - LARDAS & PARTNERS

LAW FIRM

Ranked No 1 in Greece for 6th consecutive year

in

Telecoms, Media, Technology (TMT - including Data Protection) and Intellectual Property

Also, leading / recommended firm in
Competition Law, Energy, Tax, Litigation and Employment

For more information,
please follow the link: www.nllaw.gr

Agenda

Overview

- ✓ General Background
- ✓ Major Principles
- ✓ The Team - Credentials
- ✓ Compliance Process
- ✓ May 2018 Checklist

Project Outline

- ✓ Legal Review
- ✓ Interviews
- ✓ Record of Processing Activities
- ✓ GDPR Gap Analysis

What is GDPR and what are the key changes it brings?

What is the General Data Protection Regulation (GDPR)

- GDPR is the new EU data protection framework, published in 2016, entering in force 25 May 2018
- Consists of a set of data protection rules, directly applicable to the processing of personal data across EU Member States
- Applies to any information related to an identified or identifiable living individual.

GDPR changes relevant to your Group

- **Higher degree of "accountability" & compliance requirements**
  - Keep up-to-date register of all data processing activities within the organization
  - Conduct Data Protection Impact Assessments for high-risk processing activities
  - Reviewing policies & Procedures to reflect all principles of processing and address appropriately data subjects' requests
  - Appoint a data protection officer (DPO)
  - Key point: Being compliant is no longer enough – You need to be able to demonstrate compliance
- **New framework for processing and protection of personal data**
  - Requirement to define and register legal basis & purpose of each processing activity
  - Enhanced transparency obligations
  - Data minimization – accuracy – storage limitation
  - New requirements for unambiguous & granular consent of data subjects
  - New and powerful rights for individuals (right to be forgotten, data portability etc)
  - Early determination of personal data protection measures at the data processing design stage
  - New standards govern your contractual & business relations with third parties (Controllers/processors)
  - Notification obligations in case of personal data breaches
- **Dramatic increase in regulatory risk – tougher sanctions**
  - Significantly Increased penalties for non-compliance to the greater of €20M or 4% of annual global turnover
  - Supervising authorities (DPA) with greater investigative and controlling powers (incl. audits, requests for data sharing etc)

Definition of personal data

- ‘**Personal Data**’ means any information relating to an identified or identifiable natural person (‘data subject’). A person is identifiable when it can directly or indirectly be identified, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to other factors specific to the identity of that person.
- Processing of Special Categories of data & Data related to criminal convictions and offences

Examples of “standard” personal data

- Name
- Identity / passport number
- Physical Address, contact details, email address
- Financial information (IBAN, credit card number, salary)
- Profession, experience, education
- Marital status
- Behavioral data (preferences, habits, browsing behavior)
- IP address, other unique identifiers

“Special Categories” of personal data

- Racial or ethnic origin; political opinions;
- Religious or philosophical beliefs;
- Trade union membership;
- Data concerning health or sex life and sexual orientation;
- Genetic data (new); and
- Biometric data where processed to uniquely identify a person (new).

General Background

- On December 15, 2015, the European Commission, the European Parliament, and the European Council agreed to an EU data protection reform to boost the EU Digital Single Market.
- The bill was adopted by the European Council and the European Parliament in early April 2016 and came into force on May 24, 2016 as the EU General Data Protection Regulation (the "GDPR").
- EU Regulations enjoy "**direct applicability**" (**direct effect**): the rule is that they are "immediately applicable" and they don't need national transposition.
- However, the GDPR provides for a two-year "grace period," and will take full legal effect as of May 25, 2018.
- The GDPR replaces the EU Data Protection Directive and constitutes a set of data protection rules that are directly applicable to the processing of personal data across EU Member States.
- The GDPR applies to data from which a living individual is identified or identifiable (by anyone), whether directly or indirectly.

Processing of Personal Data

'**Processing"** of personal data 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

Examples of "Processing Activities":

- ✓ Collection
- ✓ Recording
- ✓ Organisation, structuring
- ✓ Storage
- ✓ Adaptation or alteration
- ✓ Retrieval
- ✓ Consultation
- ✓ Use
- ✓ Disclosure by transmission / dissemination or otherwise making available
- ✓ Alignment or combination
- ✓ Restriction
- ✓ Erasure / Destruction

Important Note: Processing of "Special Categories of Personal Data" & Data related to criminal convictions and offences are subject to more stringent conditions than other forms of personal data.

Accountability Principle

Previously: obligation to notify the relevant Data Protection Authority.

The GDPR places **greater emphasis on the documentation** that data controllers must keep **to demonstrate accountability**.

This new "**accountability principle**" makes controllers responsible for demonstrating compliance with the data protection principles.

Under the GDPR, **you must not only comply with the six general principles, but also be able to demonstrate you comply with them**.

Accountability Principle

According to the concept of accountability**, companies are <u>required to document</u> their data protection governance and compliance programs**. In practice, companies have to:

- ❑keep an **up-to-date register of all data processing** within their organization,
- ❑conduct **privacy impact assessments** for data processing presenting high risk for the protection of personal data,
- ❑adopt **policies to handle appropriately data subjects' requests**, and
- ❑Subject to certain conditions, appoint a **data protection officer** (**DPO**).

Processing Conditions

The processing of personal data will only be lawful if it satisfies at least one of the following processing conditions:

- **Consent** - The individual has given consent to the processing for one or more specific purposes. Consent will be much harder to obtain under the GDPR.
- **Necessary for performance of a contract** - The processing is necessary for the performance of a contract with the individual or in order to take steps at the request of the individual prior to entering into a contract.
- **Legal obligation** - The processing is necessary for compliance with a legal obligation to which the controller is subject. Only legal obligations under European Union or Member State law will satisfy this condition.
- **Vital interests** - The processing is necessary in order to protect the vital interests of the individual or of another natural person. This is typically limited to processing needed for medical emergencies.
- **Public functions** - The 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.
- **Legitimate interests** - The 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.

The six general principles

A controller must ensure the processing of personal data complies with all six of the following general principles:

- **Lawfulness, fairness and transparency** - Personal data must be processed lawfully, fairly and in a transparent manner;
- **Purpose limitation** - Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (with exceptions for public interest, scientific, historical or statistical purposes);
- **Data minimisation** - Personal data must be adequate, relevant and limited to what is necessary in relation to purposes for which they are processed;
- **Accuracy/data quality** - Personal data must be accurate and, where necessary, kept up to date. Inaccurate personal data to be erased or rectified without delay.
- **Retention** - Personal data should be kept in an identifiable format for no longer than is necessary (with exceptions for public interest, scientific, historical or statistical purposes); and
- **Integrity and confidentiality** - Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss destruction or damage, using appropriate technical or organisational measures.

Data Breach Notification Obligation

✓ Notification obligations (to supervisory authorities and to data subjects) are potentially triggered by “accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data”.

✓It only **captures actual breaches** and **not suspected breaches**.

✓The GDPR requires data controllers to provide notice of serious security breaches to the competent Data Protection Authority/ies ("DPA(s)") without undue delay and, in any event, **within 72 hours after having become aware of any such breach**.

✓The inclusion of this obligation places a significant burden on companies, which will be under time constraints to carry out an assessment of the scope and breadth of the breach. In certain circumstances, data controllers may be bound to inform data subjects about such a breach.

✓A **failure to report a breach** when required to do so could **result in a fine**, as well as a **fine for the breach itself**.

Administrative Fines – Broad investigative and corrective powers

Supervisory authorities (such as the DPA in Greece) enjoy wide investigative and corrective powers including the power:

- to impose **administrative fines of up to €20,000,000 or 4% of annual global turnover**, whichever is the higher.
- to undertake **on-site data protection investigations and audits**
- to order controllers and processors to provide information;
- to obtain from controllers or processors access to personal data and other information;
- to issue public **warnings** and **orders** to carry out specific remediation activities (e.g. to order controllers/ processors to bring processing operations into compliance with the GDPR; or to order controllers to communicate personal data breaches to data subjects).

The team

- Legal and compliance experts with deep (and proven) **knowledge of data protection and cybersecurity** matters.
- Legal and compliance experts, **ranked Tier 1 for 6 consecutive years**.
- Experienced consultants co-operating with international law firms
- **Certified professionals**.
- Representing - **for 20 years** - companies before Regulatory Authorities (DPA, EETT, ADAE) and Administrative courts – **Agency Litigation**

Design and implement Data Security and Governance Systems of high quality

Transfer regulatory requirements to efficient Technical Solutions

Plan and execute technical Projects of large size and complexity

Provide creative consulting in business transformation.

Successfully represent clients before governmental agencies,

nl & partners / Nikolinakos – Lardas & Partners Law Firm

- Top Tier and Leading Law Firm in TMT and Data Protection
- **Ranked No 1** in Greece for the **6th consecutive year** in TMT – including Data Protection, [Legal500, EMEA]
- Co-operation with international law firms, such as Bird & Bird; Gibson Dunn; Dentons; Osborne Clarke; Orrick; etc.

- Key senior legal counsels participating in the GDPR legal/compliance team are:
  - **Dr. Nikos Nikolinakos**, Managing Partner, Head of Digital Business Practice Group
  - **Ms Dina Kouvelou** (Partner and Head of Data Protection & Cybersecurity Practice)
  - **Mr John Giannakakis** (Partner and co-head of Data Protection & Cybersecurity Practice) – DPO ACADEMY (Nomiki Vivliothiki & TUV Austria)
  - **Mr Alexis Spyropoulos** (Of Counsel, former head of Legal Department at the E.E.T.T. – Hellenic Telecommunications & Postal Commission)

May 2018 Checklist

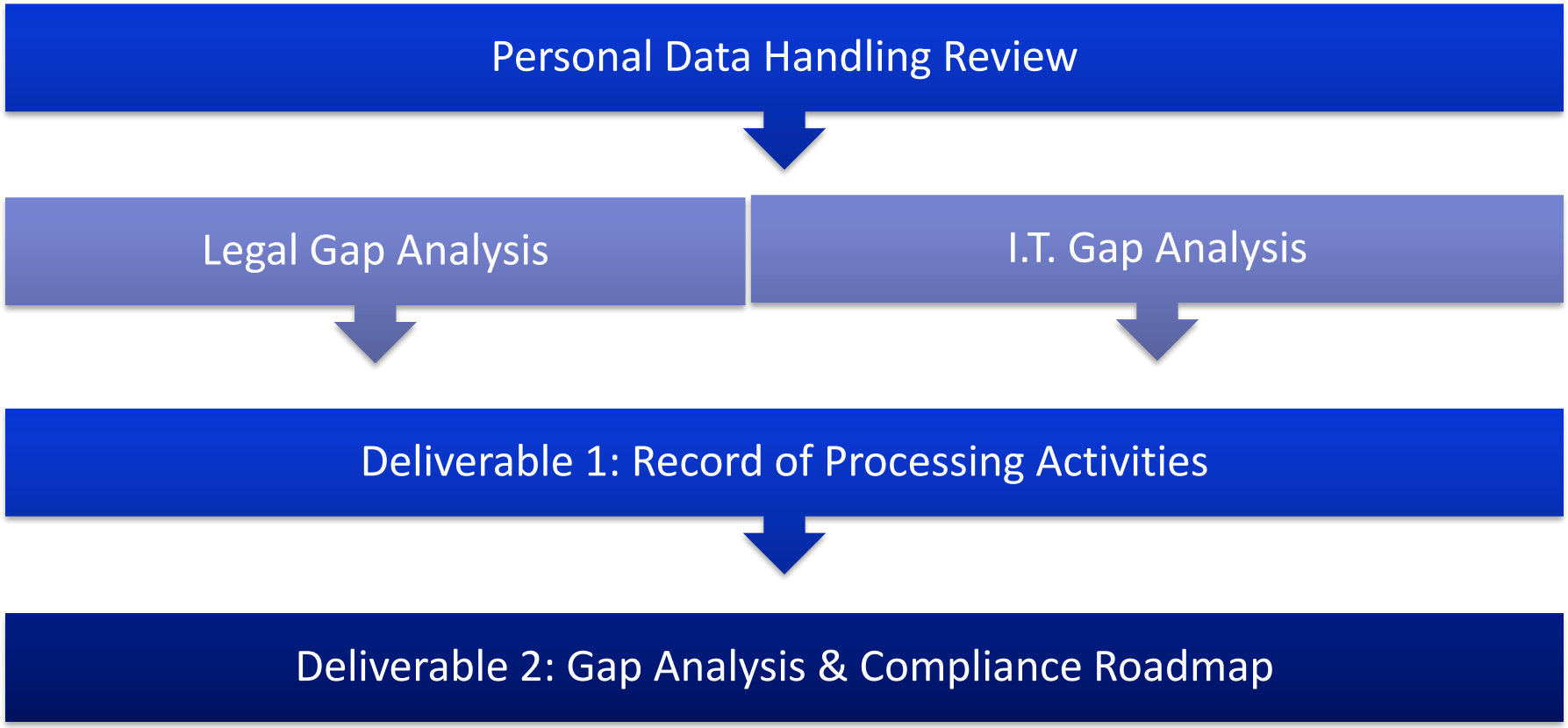
Have in place

- Data Protection Officer
- Record of Processing Activities
- Privacy Impact Assessment
- Security measures
- Business Continuity Plan
- Incident Response Plans
- Updated processes/systems to comply with GDPR
- Updated documentation (NDAs, Contracts, Forms)

Be able to respond to

- Right to access
- Right to rectification
- Right to erasure
- Right to restriction of processing
- Right to data portability
- Right to object

GDPR Compliance Preparation Project



Interviews

- Defining the right participants
- Separate Interviews with each function's representatives.
- Questionnaires:

  We use 2 types of forms/questionnaires to guide the discussion through the interviews:

  i. Questionnaire with all required fields for the Record of Processing Activities
  ii. Additional questions covering a) generic data governance issues and b) information required for compliance gap analysis per each processing activity

  If necessary – depending on the volume of information and your team's availability – the two categories of forms/questionnaires can be reviewed in more than one interviews with each function.

  - Two consultants in each interview to avoid distraction & ensure "second view".
  - Confirmation of collected data at the end of the interview.

Interviews – Record of Processing Activities

Following review of material provided, we will conduct interviews with representatives of all functions to collect information on all personal data processing activities. The purpose is to identify these activities and include in the Record information on:

- ❑Procedure involving personal data processing
- ❑Type of data processed
- ❑Purpose of Processing
- ❑Role of CCC (Data Controller / Data Processor)
- ❑Personal or Sensitive Personal Data
- ❑Legal Basis of Processing
- ❑Retention Period
- ❑Transfer to non-EEA Countries
- ❑Access Rights
- ❑Security measures to ensure data protection

Interviews – Gap Analysis

- Following the completion of the Record of Processing Activities, we identify the provisions of the GDPR applicable to your organisation.

- We conduct interviews, guided by Questionnaires which cover all applicable GDPR provisions to cover all issues not covered by documents/material provided in the first phase of the project or to get clarifications on reviewed documents, procedures, policies, contracts.

- Documents & input from interviews are analysed to produce the final deliverable on Gap Analysis and a Compliance Roadmap with proposed actions to achieve full GDPR compliance.

Legal & Compliance Gap Analysis

Legal & Compliance Audit consists of the review of:

1. Documentation collected after the kick-off meeting
   - Procedures, Policies
   - Employment contracts, customer contracts, consent forms
   - Intra-Group Agreements,
   - Supply contracts, data controller/data processor contracts

2. Information Collected through the interviews
   - Review legal basis of each processing activity
   - Review role of the organisation in each processing activity (controller/processor)
   - Review compliance of data processing activities with the principles of lawfulness', 'fairness' and 'transparency', the processing 'purpose limitation', the 'data minimisation', the personal data 'storage limitation';
   - Review appropriateness of technical and organizational measures from a legal/compliance point of view
   - Review readiness of the organisation to respond to the data subjects' rights' ('right of access' , 'right to rectification', 'right to be forgotten', 'right to restriction of processing', the 'right to data portability', 'right to object').

Deliverable 1 - Record of Processing Activities

Article 30 of the GDPR defines the mandatory fields to be included in the Record of Processing Activities. However, we see this Record not as an obligation, but as an extremely useful tool to be used on an on-going basis for compliance monitoring. Our template record is based on the form recommended by CNIL. This consists of:

i) a list of all processing activites with a unique identifier for each activity (Ref.number) and basic information on each activity

ii) An analytical register per activity, including:

-all information required by Art.30 of the GDPR

- additional information enabling on-going compliance monitoring of each activity (e.g. responsible person, defined by role, which clearly allocates responsibility for updating relevant process and allows efficiency in future reviews)

- gap analysis per processing activity (see "Gap Analysis" for further information).

Deliverable 2- Gap Analysis & Compliance Roadmap

Part 1: Data Governance Gap Analysis

Review of Organisation's Data Governance versus GDPR, indicatively:

- Required roles, with clear mandate (including applicability of DPO appointment obligation, fulfillment of requirements – if appointed at the time of Gap Analysis)
- Compliance Procedures – how the organisation implements on-going monitoring of GDPR compliance
- Adoption of process for Data Breach Handling & Notification
- Implementation of Privacy by Design & by Default in company procedures related to introduction of new services / new systems / new applications
- Assessment of standard clauses used in contracts with processors/controllers
- Training
- Local & Group General Data Protection Policies

Part 2: Gap Analysis Per Processing Activity

- Review of each Processing Activity's compliance with Processing Principles
- Review of Readiness to Satisfy Data Subjects' Rights

Part 3: Compliance Roadmap

Actions proposed for each identified gap.

Thank you

www.nllaw.gr