MYTILINEOS

Records of processing activities (article 30 of GDPR): a good practice in a large scale organization

PRESENTATION

AGENDA

1. The company
2. Challenges
3. The GDPR program
4. Records of processing activities:
   - Main principles
   - Contents for data controllers
   - Contents for data processors
5. Records of processing activities:
   - Good practice overview
   - Compliance check controllers
   - Compliance check processors
   - Database application

1. The company

- MYTILINEOS is one of Greece’s leading industrial companies, with activities in Metallurgy, EPC, Electric Power and Gas Trading.
- MYTILINEOS is listed on the Athens Exchange since 1995. Today, the Company's stock is a constituent of the FTSE 25 Large Capitalization index. In the last years, the Company has significantly increase its turnover and profits, and its activities have substantially contributed to infrastructure creation across the country.
- MYTILINEOS is a global leader in the EPC sector (Engineering-Procurement-Construction) through METKA. The Company specializes in the construction of power plants from design and procurement through to construction and completion, and has achieved an unprecedented penetration in developing markets abroad, with projects concurrently underway in Europe, Turkey, the Middle East, Asia and North Africa, constituting it as one of Greece’s leading exporting companies.
- Today, the Company is a frontrunner in the Metallurgy sector. MYTILINEOS owns ALUMINIUM OF GREECE, the largest vertically integrated aluminum and alumina producer in the European Union, and one of the most robustly growing industrial businesses in Greece.

2. Challenges

- **Large scale organization** with:
  - Many business units in various scope of services: EPC, Metallurgy, Power and Gas trading
  - International presence including jurisdictions with loose or no data privacy regulations and needs for data transfer activities
  - More than 2,700 **employees** working on hundreds of programs/ projects
- **Multiple IT systems** and applications that contain personal data
- Data processing takes place for our **customers** and end users
- Data processing **subcontracted** to selected providers

3. The GDPR program

- Protecting the security and privacy of personal data of related stakeholders (employees, customers, suppliers, vendors and partners) is important to Mytilineos S.A. Therefore, all personal data is processed in compliance with applicable laws on data protection and data security.
- Mytilineos S.A. has engaged in the new GDPR by:
  - Setting up a **competent DP organization** (Steering Committee, DPO, project group)
  - Drafting of the relevant **policies and guidelines**
  - Conducting the **employee training**
  - Identifying and **mapping of all assets** containing personal data with continuous monitoring and updates
  - Revising the **Technical and operational measures** (TOMs)
  - Conducting **Data privacy impact assessments** (DPIAs)
  - Revising data **deletion concepts**
  - Clearly identifying the **Legal basis for data processing**
  - Setting up measures for **monitoring of the subcontracted activities**
  - Establishing a **reporting mechanism** to the relevant authority

4. Records of processing activities (article 30): Main principles

- **Discontinued** obligation to send **notification to the data protection authority** in regards to the processing activities.
- Obligation for the controller as well as for the data processor to **maintain a record of the processing activities** under their responsibility.
- The **obligation shall not apply** to an enterprise or an organisation employing fewer than 250 persons unless:
  - the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects,
  - the processing is not occasional, or
  - the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.
- The controller or the processor and, where applicable, the controller's or the processor's representative, shall **make the record available to the supervisory authority** on request.

4. Records of processing activities: Contents for data controllers

- The **data controller** records should contain:
    - WHO: the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer
    - WHY: the purposes of the processing
    - WHAT: a description of the categories of data subjects and of the categories of personal data
    - TO WHOM: the categories of recipients to whom the personal data has been or will be disclosed including recipients in third countries or international organisations
    - TRANSFERS (to 3rd countries): where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards
    - HOW LONG: where possible, the envisaged time limits for erasure of the different categories of data
    - HOW: where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

4. Records of processing activities: Contents for data processors

- The **data processor** records should contain:
  - WHO: the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer
  - WHAT: the categories of processing carried out on behalf of each controller;
  - TRANSFERS (to 3rd countries): where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards
  - HOW: where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

5. Records of processing activities: Good practice overview

- **Organizational setup:** Identify key internal stakeholders (sales, legal, HR, IT, Marketing, compliance), nomination of project lead [Data Privacy Officer or Data Privacy Manager]
- **Engage:** Kick off meeting to present project plan, roadmap and key activities/role for each key stakeholder
- **Conduct Interviews/ workshops:** to identify all processing activities that contain personal data
  - Schedule interview meetings per business area
  - Train: create awareness on the GDPR and the definitions (processing activity, controller, processor, transfer etc.)
  - Ask input on personal data processing activities (internal local IT applications, internal central IT applications, hardcopies/ manual processing, outsourced processing, security cameras, visitor logbook etc.)
- **Categorize** processing activities and bundle, where necessary, acc. to the purpose
- **Record** processing activities in database
- Conduct **gap analysis** on input against the new GDPR (Compliance check).
- Establish a process for **recording new** data processing.
- Establish a **continuous update** process of records in case of changes, nominate contact person

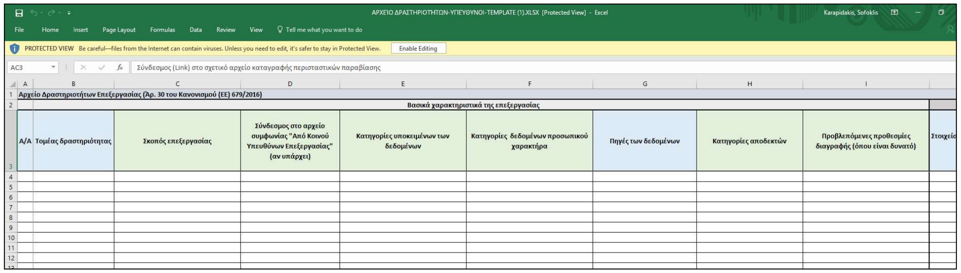
5. Records of processing activities: Compliance check controllers

- Conduct **gap analysis** on input against the new GDPR principles (Compliance check) for **controllers** per processing purpose:
  - Is the processing **purpose** clear? (lawfulness, fairness and transparency)
  - Is the processing performed only for the identified purpose? (purpose limitation)
  - How has the data been **collected**? (e.g. directly, indirectly, for the specific purpose)
  - Check the **legal basis** under which the data are being processed (consent, contractual agreement, legal obligation, vital interests of the data subject, public interest, legitimate interests pursued by the controller article 6 par.1)
  - Is the data adequate, relevant and **limited to what is necessary** in relation to the purpose? (data minimisation)
  - Is the data **accurate**? (accuracy)
  - Are the appropriate **technical and operational measures** in place for the security of the data? (integrity and confidentiality)
  - Do the **cooperating organizations** (subcontractors) provide the necessary compliance to the GDPR?
  - Is the controller responsible for and able to demonstrate compliance with the above? (accountability)

5. Records of processing activities: Compliance check processors

- Conduct **gap analysis** on input against the new GDPR (Compliance check) for **processors** per processing purpose:
  - Is the processing exclusively based on the documented **instructions by the data controller**?
  - Any **further processing** of the data, other than the designated purpose under the initiative of the processor, places the latter one as controller and is constitutes a violation.
  - Have the employees that carry the processing signed confidentiality clauses?

6. Records of processing activities: excel based application



ΑΡΧΕΙΟ ΔΡΑΣΤΗΡΙΟΤΗΤΩΝ-ΥΠΕΥΘΥΝΟΙ-TEMPLATE (1).XLSX [Protected View] - Excel

Karapidakis, Sofoklis

PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

AC3 Σύνδεσμος (Link) στο σχετικό αρχείο καταγραφής περιστατικών παραβίασης

	A	B	C	D	E	F	G	H	I	
1	Αρχείο Δραστηριοτήτων Επεξεργασίας (Άρ. 30 του Κανονισμού (ΕΕ) 679/2016)									
2		Βασικά χαρακτηριστικά της επεξεργασίας								
3	Α/Α	Τομέας δραστηριότητας	Σκοπός επεξεργασίας	Σύνδεσμος στο αρχείο συμφωνίας "Από Κοινού Υπευθύνων Επεξεργασίας" (αν υπάρχει)	Κατηγορίες υποκειμένων των δεδομένων	Κατηγορίες δεδομένων προσωπικού χαρακτήρα	Πηγές των δεδομένων	Κατηγορίες αποδεκτών	Προβλεπόμενες προθεσμίες διαγραφής (όπου είναι δυνατό)	Στοιχεία
4										
5										
6										
7										
8										
9										
10										
11										

Βασικά χαρακτηριστικά επεξεργασίας

- Τομέας δραστηριότητας
- Σκοπός επεξεργασίας
- Σύνδεσμος στο αρχείο συμφωνίας "Από Κοινού Υπευθύνων Επεξεργασίας" (αν υπάρχει)
- Κατηγορίες υποκειμένων των δεδομένων
- Κατηγορίες δεδομένων προσωπικού χαρακτήρα
- Πηγές των δεδομένων
- Κατηγορίες αποδεκτών
- Προβλεπόμενες προθεσμίες διαγραφής (όπου είναι δυνατό)

Εκτελούντες την Επεξεργασία

- Στοιχεία Εκτελούντα την επεξεργασία (αν υπάρχει)
- Σύνδεσμος στο αρχείο της σύμβασης με εκτελούντα την επεξεργασία

Διαβιβάσεις σε 3ες χώρες

- Τρίτες χώρες ή διεθνείς οργανισμοί στους οποίους θα διαβιβαστούν τα δεδομένα (εφόσον υπάρχουν)
- Νομική Βάση για τη διαβίβαση (σύμφωνα με άρθρα 45-49 του Κανονισμού)
- Τεκμηρίωση εγγυήσεων για τις διαβιβάσεις σε τρίτες χώρες ή διεθνείς οργανισμούς (εφόσον πραγματοποιείται διαβίβαση σύμφωνα με το άρ. 49 παρ. 1 β' εδαφ. του Κανονισμού)

Τεχνικά και οργανωτικά μέτρα

- Τόπος ή πληροφοριακό σύστημα τήρησης των δεδομένων προσωπικού χαρακτήρα
- Γενική περιγραφή οργανωτικών και τεχνικών μέτρων ασφάλειας (όπου είναι δυνατό)
- Σύνδεσμος στο αρχείο με αναλυτική περιγραφή των μέτρων ασφάλειας

Νομιμότητα της Επεξεργασίας

- Βάση για τη νομιμότητα της επεξεργασίας, σύμφωνα με το άρ. 6 του Κανονισμού
- Υπέρτερα έννομα συμφέροντα για την επεξεργασία (εφόσον η βάση για τη νομιμότητα είναι το άρ. 6 παρ. 1 στοιχ. στ')
- Βάση για τη νομιμότητα της επεξεργασίας ειδικών κατηγοριών δεδομένων, σύμφωνα με το άρ. 9 του Κανονισμού
- Τρόπος απόδειξης συγκατάθεσης (εφόσον η βάση για τη νομιμότητα είναι η συγκατάθεση)

- Δικαιώματα που παρέχονται στα υποκείμενα των δεδομένων
- Πραγματοποιείται αυτοματοποιημένη λήψη αποφάσεων, συμπεριλαμβανομένου προφίλ; (εάν έχει εφαρμογή)

DPIA

- Απαιτείται η διενέργεια εκτίμησης αντικτύπου στην προστασία προσωπικών δεδομένων (ΕΑΠΔ);
- Στάδιο (πρόοδος) στο οποίο βρίσκεται η ΕΑΠΔ
- Χρειάστηκε προηγούμενη διαβούλευση με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα;
- Σύνδεσμος (Link) στο κείμενο της ΕΑΠΔ

Περιστατικά παραβίασης

- Έχει λάβει χώρα περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα;
- Σύνδεσμος (Link) στο σχετικό αρχείο καταγραφής περιστατικών παραβίασης

Source: http://www.dpa.gr/portal/page?_pageid=33,211400&_dad=portal&_schema=PORTAL

6. Records of processing activities: Database application

- **Record** processing activities in database
- Database application used as a **process flow to detail each of the applications** in regards to the below fields:
  - **General** information (name of application, asset description)
  - **Purpose** of the processing (assignment to specific categories: IT admin, Manufacturing, HR, procurement, sales, service)
  - **Categories** of data stored (employee, customer, supplier, 3rd party data- Data categories: normal/ special)
  - **Legal basis** for the processing (consent, contractual agreement, legal obligation, vital interests of the data subject, public interest, legitimate interests pursued by the controller)
  - Use of data **processors** (listing of names/ countries)
  - Data **transfer** (listing of recipients/ countries)
  - **Authorized** persons/ groups
  - **Deletion** concept
  - **Technical and operational measures**
  - **Data Privacy Impact assessment** (DPIA)
  - Versioning **log**

THANK YOU

Sofoklis Karapidakis

Compliance Director

mytilineos.gr