MAY 2018

EUROMETAUX GDPR DATA PROTECTION IMPACT ASSESSMENT

PIA

Eurometaux general communication – membership and subscriptions

Author's name

Guy Thiran

Assessor's name

Guy Thiran

Creation date

11/05/2018

Context

Overview

Which is the processing under consideration?

Membership and partners, registered stakeholders for grouped information and mailing, invitation to events, newsletters

What are the responsibilities linked to the processing?

Accuracy of the information, non-disclosure outside of the organisation, right of access, modification or removal of any data. Eurometaux acting as data owner and controller

Are there standards applicable to the processing?

Eurometaux data privacy policy. Prior informed consent of information / invitation recipients. Salesforce automated distribution.

Data, processes and supporting assets

What are the data processed?

Name, first name, e-mail, organisation (member companies and national association), Eurometaux committee, WG and TF membership (for targeted invitation or information only to members) social media accounts as available.

MAY 2018

How does the life cycle of data and processes work?

Professional data kept as long as the contact person is designated or authorised stakeholder by its organisation automated e-mail or mailing to member and affiliated companies, partners and EU stakeholders that provided their PIC

What are the data supporting assets?

Salesforce Customer Relations Management system.

Fundamental principles

Proportionality and necessity

Are the processing purposes specified, explicit and legitimate?

Yes – as per Eurometaux data privacy policy

What are the legal basis making the processing lawful?

Legitimate purpose of the data processing for Eurometaux missions, GDPR (PIC)

Are the data collected adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')?

Exclusively processing relevant professional data for e-mailing and occasionally postal mails. Twitters accounts for targeting postings to members / interested stakeholders or monitoring social media activities

Are the data accurate and kept up to date?

Yes. D-base regularly updated

What are the storage duration of the data?

As long as the person is a designated / authorised stakeholder of a company or association in relation with Eurometaux. Typically linked to a company membership in Eurometaux member associations, a partnership or the registration to subscribed content or participation in a Eurometaux committee, working group or task force

Controls to protect the personal rights of data subjects

How are the data subjects informed on the processing?

Privacy policy, prior informed consent for mass-communication

If applicable, how is the consent of data subjects obtained?

Request to sign up for invitation, newsletter / information as part of explicit PIC for data processing

Eurometaux - European Association of Metals
Avenue de Broqueville 12 | B-1150 Brussels | Tel: +32 (2) 775 63 11 | www.eurometaux.eu | eurometaux@eurometaux.be | @Eurometaux

MAY 2018

How can data subjects exercise their rights of access and to data portability?

Directly contacting Eurometaux data controller via e-mail addressed to datacontroller@eurometaux.be

How can data subjects exercise their rights to rectification and erasure?

Directly contacting Eurometaux data controller via e-mail addressed to datacontroller@eurometaux.be

How can data subjects exercise their rights to restriction and to object?

Directly contacting Eurometaux data controller via e-mail link addressed to datacontroller@eurometaux.be

Are the obligations of the processors clearly identified and governed by a contract?

Data are processed by Eurometaux according to Privacy Policy. Data not shared to third parties or for any commercial use.

In the case of data transfer outside the European Union, are the data adequately protected?

Not relevant.

Risks

Planned or existing measures

Restricted access to d-base

The d-base and processing activities are only accessible by Eurometaux employees through secured access to network. Mailings and invitation are sent by Eurometaux staff only for legitimate use only.

Illegitimate access to data

What could be the main impacts on the data subjects if the risk were to occur?

access to name, e-mail and professional address of contacts. No sensitive information contained. Main risk identified is the use of Eurometaux contact base for phishing

What are the main threats that could lead to the risk?

Phishing

What are the risk sources?

External attempt to access d-base; employee misuse of d-base

Which of the identified controls contribute to addressing the risk?

Eurometaux - European Association of Metals
Avenue de Broqueville 12 | B-1150 Brussels | Tel: +32 (2) 775 63 11 | www.eurometaux.eu | eurometaux@eurometaux.be | @Eurometaux

MAY 2018

Restricted access to d-base, tightening of passwords and staff briefing on data privacy policy and practices, CRM training of employees.

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Limited, controlled through IT security checks.

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Limited, Usual attempts to break into Eurometaux server but IT security and measures in place to prevent (and access to d-base secured).

Unwanted modification of data

What could be the main impacts on the data subjects if the risk were to occur?

Unwanted e-mail, phishing

What are the main threats that could lead to the risk?

Phishing

What are the risk sources?

External

Which of the identified controls contribute to addressing the risk?

Restricted access to d-base (Eurometaux staff only) and controlled through IT security checks

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Limited, controlled through IT security checks

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Limited.

Data disappearance

What could be the main impacts on the data subjects if the risk were to occur?

Requiring new PIC and contact details, e-mails, restricted access to subscribed content, invoicing (accounting) and mailing

MAY 2018

What are the main threats that could lead to the risk?

External hacking

What are the risk sources?

External hacking

Which of the identified controls contribute to addressing the risk?

Restricted access to d-base (Eurometaux staff only) and controlled through IT security checks, systematic daily back-up

How do you estimate the risk severity, especially according to potential impacts and planned controls?

Negligible

How do you estimate the likelihood of the risk, especially in respect of threats, sources of risk and planned controls?

Negligible.

Action plan

Fundamental principles

No action plan required.

Existing or planned measures

IT security and privacy policy – GDPR staff training - Control and monitoring of access to d-base

Risks

Limited.

Eurometaux - European Association of Metals
Avenue de Broqueville 12 | B-1150 Brussels | Tel: +32 (2) 775 63 11 | www.eurometaux.eu | eurometaux@eurometaux.be | @Eurometaux