DATA BREACH REPORT

EuroCloud Europe will undertake to create a European database of data-breach-related DPA decisions and court judgments.

This report presents the key findings and recommendations on data breach-related obligations in the EU/EEA as determined by a comparative survey conducted by 13 members of the EuroCloud Europe Cloud Privacy Check Network (hereinafter: "CPC Network") along with the action plan of the CPC Network for 2019. Author: Mary Deligianni, Zepos & Yannopoulos, Greek member of the EuroCloud Europe CPC Network

1. Procedure for reporting personal data breaches to the Data Protection Authorities (DPAs)

The vast majority of DPAs have issued standard forms for the reporting of personal data breaches. The survey shows that all such notification forms are available online, are drafted in the official language of the respective EU/EEA country, and must be submitted online or by email. In terms of contents, however, they require additional information compared to what is mandated by the GDPR. For transparency and efficiency purposes, the CPC Network would welcome a uniform data breach notification form to be used by all EU/EEA DPAs, preferably available also in English.

2. Contractual arrangements in data processing agreements

The CPC Network proposes that all data processing agreements, when regarded from the perspective of the controller, should include a provision detailing the obligations of the processor in the event of a personal data breach occurring in the IT systems and/or files of the processor or its sub-processors. The processor should ideally undertake:

(a) To notify in writing the controller within 24 hours of its knowledge of the breach. This notification should include specific information as detailed in the agreement so that the controller can fully report the breach to the DPA and inform the affected individuals.

(b) To immediately take all actions necessary to investigate and address the breach, minimize adverse effects, and prevent or restrict further dissemination of the leaked personal data.

(c) To keep the data breach confidential and commit to not disclosing or publishing any notice, press release, or report to the data subjects, the DPA, or third parties without the controller's approval.

(d) In general, to assist the controller to ensure compliance with its obligations relating to data breaches as per the applicable data protection laws.

With regard to liability, the CPC Network is of the opinion that the controller should be entitled to request from the processor compensation for any direct damages, loss of profit and/or reputation, including any administrative fines imposed by the DPA or other regulatory authority.

3. Action plan for 2019

The CPC Network intends to gather information on the volume, type and business sectors of occurring data breaches as well as the regulatory response to data breach notifications, and to draft a relevant report. Furthermore, to the extent it is possible, the CPC Network will undertake to create a concise database of data-breach-related DPA decisions and court judgments.

ABOUT CPC

Following the advancement of European data protection legislation with the entering into force of the GDPR, the elimination of geo-blocking, and the establishment of the ePrivacy framework and the new Electronic Communications Code, it may be expected that businesses, regulators, individuals, and advisors will enter a new era of treating data flows and data protection.

Having considered these trends, CPC - comprising experts from more than 30 European countries - established a network of independent lawyers, IT specialists, advertising experts and media with the aim of analysing and guiding the practical impact of this evolution of European practice in applying the various regulations relating to data, and especially to personal data.

As a result, the CPC Network was founded by EuroCloud Europe in 2015 with the main focus of identifying simplified solutions for dealing with data in a cloud environment and making them available to the public. The CPC is a trusted, not-for-profit international network of qualified legal professionals who deliver simplified and straight-forward guidance to help navigate the legal and regulatory environment relating to privacy and the cloud. This is done through collective know-how, research and market analysis gained from pan-European industry activity, collaboration and experience. The mission is to provide authoritative views, information and practical solutions to two principal stakeholders: industry professionals and public authorities.

Over the past years, the CPC Network has compiled and released more than 200 short treatises dedicated to improving understanding of legal and practical aspects of data, technology, and the relation between them. In addition, the CPC Network has launched the Internet platform www.cloudprivacycheck.eu, as part of https://eurocloud.org an independent web resource dedicated to another way of optimizing the time of all people involved with data protection—namely to understanding data transfers in the cloud in four simple and easily identifiable steps. The above material has attracted several hundred thousand readers from all over the world.

The CPC Network's plan for 2019 is to further elaborate on certain practical aspects of data protection. A CPC group tentatively entitled "Joint Controllers and Processors as per the GDPR" is in the process of drafting materials covering case studies in various industries as well as some thoughts on how to treat different business flows from a data protection perspective.

The main idea of this group is to identify and explain various issues caused by the assignment of roles in a data processing relationship with multiple participants. In its preliminary studies, the group has come to the conclusion that a unified approach cannot be adopted and that each such relationship must be dealt with on an individual basis.

The group is seeking appropriate mechanisms to propose the compilation of guidance documents to make it easier for companies to settle their role assignments when dealing with a controller-processor or joint controller relationship.

A second CPC-Sup-group of EuroCloud Europe will undertake to create a European database of data-breach-related DPA decisions and court judgments. The CPC Network intends to gather information on the volume, type and business sectors of occurring data breaches as well as the regulatory response to data breach notifications, and to draft a relevant report. Furthermore, to the extent it is possible, the CPC Network will undertake to create a concise database of data-breach-related DPA decisions and court judgments.

CPC members: https://cloudprivacycheck.eu/who/