Ogee Technologies

WWW.OGEETECH.COM

Thoughts – Vol. 02

April 2019

IN THIS ISSUE

THINGS TO KNOW ABOUT PESONAL DATA BREACH NOTIFICATION

Personal data breach: Personal data breach is, a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or processed.

When there is a data breach, the entity shall trigger an incident management and response mechanism that enables to respond quickly and effectively as a result the impacts of such breaches could be minimized

Notification: The GDPR has specific rules regarding when and how an incident must be reported to the supervisory authority and to the affected data subjects.

BACKGROUND

Data Controller: Determines the purpose and means of data processing. Ensures effective and complete protection of Data Subjects.

Data Processor: Who processes personal data on behalf of a controller without determining the purpose and means of the processing.

Data Controller and Data Processor shall adhere to demonstrate their compliance with the GDPR requirements.

Data Subjects: Identified or identifiable natural living person, whose data are being processed in line with the territorial scope article 3 of GDPR.

Data Subject Rights: GDPR proposes a set of rules that are meant to help data subjects and enforce their rights against abusive personal data processing.

Data subjects may complain to the regulator where they believe a breach of the GDPR takes place and may also issue legal proceedings against controllers and processors.

Notification of the personal data breach to the Supervisory Authority:

The data controller is required to notify the supervisory authority as soon as the controller becomes aware of the personal data breach, without any undue delay and, where feasible, not later than 72 hours after having become aware of the personal data breach.

The processor shall notify the data controller without any undue delay after becoming aware of the personal data breach

It is good practice to make notifications to the supervisory authority by default, in order to avoid accidentally breaking the law

(*even if the personal data breach is unlikely to result in a risk to the rights and freedoms of natural person*)

The notification to the Supervisory authority shall include:

a. Description of the nature of the personal data breach
b. Categories and approximate number of data subjects concerned
c. Categories and approximate number of personal data records concerned
d. The name and contact details of the Data Protection Officer (DPO)
e. Other contact point where more information can be obtained
f. The likely consequences of the personal data breach
g. The measures taken or proposed to be taken by the data controller
h. Appropriate measures to mitigate possible adverse effects

The communication of the personal data breach to the data subjects **shall not be required** if any of the following conditions are met

a. Appropriate technical and organizational protection measures were applied to the personal data affected, that render personal data unintelligible to any person who is not authorized to access.
b. The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize
c. It would involve disappropriate effort to contact individuals, where their contact details have been lost as a result of the breach or not known, in such a case there shall be a public communication or similar measure that data subjects are informed in an equally effective manner.

The communication of the personal data breach to the data subjects shall include:

a. Describe in clear and plain language the nature of personal data breach
b. Describe the likely consequences of the personal data breach
c. Describe the measures taken or proposed to be taken by the controller to mitigate its possible adverse effects
d. Communicate the name and contact details of the DPO

There are two levels of fines based on the GDPR

1. GDPR sets forth the lower level of fines up to 10 million euros, or, in the case of an undertaking, up to 2% of its entire global turnover of the preceding fiscal year, whichever is higher.
   This includes infringements relating to:
   - Integrating data protection 'by design and by default'
   - Records of processing activities
   - Co-operation with the supervising authority
   - Security of processing data
   - Notification of a personal data breach to the supervisory authority
   - Communication of a personal data breach to the data subject
   - Data Protection Impact Assessment
   - Prior consultation with SA for processing resulting in High risk
   - Designation, position or tasks of the Data Protection Officer
   - Conditions for children's consent

Infringements and Administrative Fines

The fines are applied in addition to, further remedies or corrective powers, such as the order to end a violation, an instruction to adjust the data processing to comply with the GDPR, as well as impose a temporary or definitive limitation including a ban on data processing.

The fines are applicable to both data controllers and data processors. The fines must be effective, proportionate and dissuasive for each individual case.

- Processing that doesn't require identification
- General obligations of processors and controllers
- Certification and Certification bodies

2. GDPR sets forth the higher level of fines up to 20 million euros, or in the case of an undertaking, up to 4 % of their total global turnover of the preceding fiscal year, whichever is higher.
   This includes infringements relating to:
   - Data processing principles
   - Lawful bases for processing
   - Conditions for consent
   - Processing of special categories of data
   - Data subjects' rights
   - Data transfers to third countries
   - Intentional infringement
   - Failure to take measures to mitigate the damage

Determination for application of administrative fines

Fines are administered by individual member state supervisory authorities. The ten criteria are used to determine the amount of the fine on a non-compliant firm

1. **Nature of infringement:** The nature, gravity and duration of the infringement, number of people affected, damaged they suffered, duration of infringement, scope or purpose of processing
2. **Intention**: Whether the infringement is intentional or negligent
3. **Mitigation**: Actions taken by the controller to mitigate damage to data subjects
4. **Preventative measures:** The degree of responsibility of the controller or processor**,** technical and organizational measures the firm had previously implemented to prevent non-compliance
5. **History**: Any relevant previous infringements by the controller or processor, past administrative corrective actions under the GDPR, from warnings to bans on processing and fines
6. **Co-operation**: The degree of co-operation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement
7. **Data type**: The categories of personal data affected by the infringement

Ogee Technologies Private Limited
www.ogeetech.com
India: +91 818181 2289
Europe: +46 72973 8181
USA: +1 646 493 4478
Email: support@ogeetech.com
Skype: ogeetech_girish
Hangouts: ogeetechnologies

8. **Notification**: Whether the infringement was proactively reported to the supervisory authority by the firm itself or by a third party
9. **Certification**: Whether the firm had qualified under approved certifications or adhered to approved codes of conduct
10. **Any other aggravating or mitigating factor:** Such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

CONCLUSION

The controllers shall provide information on action taken to data subject's request without undue delay and within one month of receipt of a request. Information and action taken in response to requests shall be free of charge.

If the controller does not take an action, controller shall inform the data subject without undue delay and within one month of receipt of the request, the reasons for not taking an action and of the possibility of lodging a complaint to the supervisory authority and seeking a judicial remedy.

References:

https://ec.europa.eu
https://eugdpr.org
https://gdpr-info.eu/
https://www.i-scoop.eu/
https://www.itgovernance.co.uk
https://eur-lex.europa.eu
https://www.gdpreu.org
https://www.gdpr.associates
https://www.whitecase.com
https://eureka.eu.com

OgeeTech®
A Strategic Inflection Point