VAIMO
CORE OF COMMERCE

GDPR FINES GUIDE

Can you afford a fine up to 4% on your company's group annual turnover?

TABLE OF CONTENTS

Vaimo AB | Tel: +46 8 452 26 50 | Rosenlundsgatan 40, 11853 Stockholm

INTRODUCTION

The General Data Protection Regulations (GDPR) will enter in force in European Union countries from 25 May 2018.

GDPR brings in new elements which organisations are required to comply with – enhanced rights for consumers, mandatory data breach reporting requirements, higher standards of consent, and significantly larger fines.

IN SUMMARY

THERE ARE 39 BREACHES OF GDPR POINTS THAT COULD LEAD TO FINES

Breaches of key GDPR provisions up to

€20M *or* **4%**

(whichever is greater)

- 20/39 of the breaches leads to HIGHER level fines - €20M or 4 %
- Controller is responsible for 14/20 of these breaches
- Controller and Processor are responsible for 6/20 of these breaches

Procedural infringements up to

€10M *or* **2%**

(whichever is greater)

- 19/39 of the breaches leads to LOWER level fines - €10M or 2%
- Controller is responsible for 7/19 of these breaches
- Processor is responsible for 1/19 of these breaches
- Controller and Processor are responsible for 11 of these breaches

Controller = You as a Vaimo Client | Processor = Vaimo | Data Subject = Your customers

Vaimo AB | Tel: +46 8 452 26 50 | Rosenlundsgatan 40, 11853 Stockholm

BACKGROUND INFORMATION ABOUT GDPR ADMINISTRATIVE FINES

Under GDPR, supervisory authorities are empowered with the ability to take enforcement action; impose sanctions for non-compliance, including the ability to issue warnings for non-compliance; carry out data protection audits; require specific remediation within a specified time frame; order erasure of data; and suspend data transfers to a third country. Most notably, supervisory authorities can impose significant administrative fines on both data controllers and data processors. Fines may be imposed instead of, or in addition to, measures that may be ordered by supervisory authorities.

A two-tiered sanctions regime will apply. Breaches of key GDPR provisions could lead to fines of up to €20 million (£17,5 million) or 4% of global annual turnover for the preceding financial year, whichever is greater, being levied by a data protection regulator. For less severe breaches, such as procedural infringements, the authorities could impose fines on organisations of up to €10m (£8.7 million) or 2% of global annual turnover, whichever is greater.

BREACH NOTIFICATION RULES

Article 33 of the GDPR provides that “in the case of a personal data breach, data controllers shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority unless the personal data breach is unlikely to result in a risk for the rights and freedoms of individuals”.

Under the GDPR, a “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 otherwise processed.”

The lead supervisory to whom the “personal data breach” should be reported to is likely to be the authority of the EU member state where the controller has its main establishment or only establishment (e.g. for organisations with their main establishment or Headquarters in the UK then this would be the Information Commissioner’s Office).

Vaimo AB | Tel: +46 8 452 26 50 | Rosenlundsgatan 40, 11853 Stockholm

If a notification is not made within 72 hours of the data breach, an organisation must give a 'reasoned justification' to the supervisory authority explaining the reason for the delay. Failure to notify within 72 hours or to provide an adequate explanation for the delay could result in fines on companies of up to €10m or 2% of global annual turnover, whichever is greater.

Organisations are also required to maintain an internal breach register used to record any personal data breaches and any actions that the organisation has taken in respect of that.

Under Article 34, where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, organisations are required to communicate the data breach together with the information set out above, in clear and plain language, to individuals affected, without undue delay. There are however some circumstances when the notification is not required, including:

1. The controller has implemented appropriate technical and organisational protection measures in respect of the personal data affected by the breach (such as encryption).
2. The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of individuals is no longer likely to arise.
3. It would involve disproportionate effort.

AGGRAVATING FACTORS TO BE TAKEN INTO CONSIDERATION

GDPR Article 83(2) lists factors to be taken into account when determining whether to impose an administrative fine and deciding on the amount of any fine to be imposed. These include:

the nature, gravity and duration of the infringement having regard to the nature, scope or purpose of the processing concerned as well as the number of data subjects and level of damage suffered by them;

whether the infringement is intentional or negligent;

actions taken by the controller or processor to mitigate the damage suffered by data subjects;

Vaimo AB | Tel: +46 8 452 26 50 | Rosenlundsgatan 40, 11853 Stockholm

the degree of responsibility of the controller or processor;

any relevant previous infringements; the degree of cooperation with the supervisory authority;

categories of personal data affected; whether the infringement was notified by the controller or processor to the supervisory authority; any previous history of enforcement action;

adherence to approved codes of conduct pursuant to Article 38 or approved certification mechanisms pursuant to Article 39; and any other aggravating or mitigating factors applicable in the circumstances e.g. financial benefits gained, losses avoided, directly or indirectly, from the infringement.

✓ **HIGH**

Art. 83(5) Infringements – subject to administrative fines up to €20 million or (for undertakings) up to 4% of total worldwide annual turnover of preceding financial year, whichever is higher.

✓ **LOW**

Art. 83(5) Infringements subject to administrative fines up to €10 million or (for undertakings) up to 2% of total worldwide annual turnover of preceding financial year, whichever is higher

Vaimo AB | Tel: +46 8 452 26 50 | Rosenlundsgatan 40, 11853 Stockholm

CONTROLLER (VAIMO CLIENT) OBLIGATIONS

ARTICLE	DESCRIPTION	LOW FINES	HIGH FINES
Art. 5	Failure to adhere to any of the six data principles relating to the processing of personal data.		✓
Art. 6	Failure to ensure the lawful processing of data based on one of the conditions outlined in Art.6 (i.e. data subject has consented to processing, or processing is necessary for the performance of a contract, to fulfil a legal obligation, to protect vital interests, on public interest grounds, or for legitimate interests of the controller or third party).		✓
Art.7	Failure to demonstrate that the data subject has consented to processing of his or her personal data or that consent is valid.		✓
Art. 8	Failure to make reasonable efforts to verify that consent is given or authorised by the holder of parental responsibility over a child who is at least 16 years old (although Member States may provide by law for a lower age of 13 years) in relation to information society services.	✓	
Art. 9	Processing of special categories of personal data (e.g. health data) when none the conditions in Art.9 have been met (e.g. explicit consent by the data subject).		✓
Art. 11	Holding personal data when the identification of the data subject is not required.	✓	
Art. 12	Failure to provide data subjects (in particular for any information addressed specifically to a child) with transparent information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, for the existence of their rights under GDPR.		✓
Art. 13	Failure to provide information required under Art.13 (e.g. the identity of the controller, the purposes for processing personal data as well as the legal basis, or the recipients of personal data) where personal data are collected from the data subject.		✓

Vaimo AB | Tel: +46 8 452 26 50 | Rosenlundsgatan 40, 11853 Stockholm

ARTICLE	DESCRIPTION	LOW FINES	HIGH FINES
Art. 14	Failure to provide information required under Art.14 (e.g. the identity of the controller, the purposes for processing personal data as well as the legal basis, or the recipients of personal data) where personal data have not been obtained from the data subject.		✓
Art. 15	Failure to comply with a right of access by the data subject for data concerning him or her.		✓
Art. 16	Failure to comply with a right to rectification in relation to inaccurate data held about a data subject.		✓
Art. 17	Failure to comply with a right to erasure without undue delay where one of the conditions outlined in Art.17 applies (e.g. where the data subject withdraws consent on which the processing is based).		✓
Art. 18	Failure to restrict processing of data when one of the conditions of Art.18 is met (e.g. where the accuracy of the personal data is contested by the data subject).		✓
Art. 19	Failure to notify recipients regarding rectification or erasure of personal data or restriction of processing in accordance with Art.16, 17 or 18.		✓
Art. 20	Failure to comply with a right to data portability in relation to data which he or she has supplied to a controller.		✓
Art. 21	Failure to comply with a right to object in circumstances where a controller is unable to demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.		✓
Art. 22	Subjecting a data subject to automated individual decision-making, including profiling, which produces legal effects concerning him or her, where the clauses in Art.22 are not valid.		✓

Vaimo AB | Tel: +46 8 452 26 50 | Rosenlundsgatan 40, 11853 Stockholm

ARTICLE	DESCRIPTION	LOW FINES	HIGH FINES
Art. 25	Failing to implement appropriate technical and organisational measures, such as pseudony misation in an effective manner, in order to protect the rights of data subjects.	✓	
Art. 26	In the case of joint data controllers, failing to take respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject.	✓	
Art. 27	Failure to designate in writing a representative in the European Union for controllers or processors not established in the Union.	✓	
Art. 28	Failure by a controller to use a processor which provides sufficient guarantees to implement appropriate technical and organisational measures to ensure the protection of the rights of the data subject. Failure to put in place controller - processor obligations (e.g. contract in writing, restrictions on subcontracting).	✓	
Art. 30	Failure to maintain a detailed record of processing activities under a controller or processor responsibility (e.g. categories of data, purpose of processing, details of external transfers).	✓	
Art. 31	Failure to cooperate with the data protection supervisory authority.	✓	
Art. 32	Failure to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (e.g. encryption, pseudonymisation, business continuity).	✓	
Art. 33	Failure to notify supervisory authority of data breaches within 72 hours or provide a satisfactory reason for the delay.	✓	
Art. 34	Failure to notify data subjects of a data breach without undue delay.	✓	
Art. 35	Failure to complete a data protection impact assessment in relation to high risk processing of personal data.	✓	

Vaimo AB | Tel: +46 8 452 26 50 | Rosenlundsgatan 40, 11853 Stockholm

ARTICLE	DESCRIPTION	LOW FINES	HIGH FINES
Art. 36	Failure to consult with the supervisory authority prior to processing data that an impact assessment indicates would result in high risk in the absence of measures to mitigate risk.		✓
Art. 37-39	Failure to appoint an independent and fully supported data protection officer.		✓
Art. 41	Failure to take appropriate action in cases of infringement of approved GDPR codes of conduct.		✓
Art. 42	Failure to adhere to Art.42 requirements relating to the implementation of data protection certification mechanisms or data protection seals and marks.		✓
Art. 44	Failure to adhere to one or more conditions in Chapter V relating to transfers of Personal Data to Third Countries (e.g. outside the European Economic Union) or International Organisations.	✓	
Art. 45	Transfers of personal data outside the EU to a country which the Commission has decided does not have an adequate level of protection.	✓	
Art. 46	Failure to ensure legal mechanism (e.g. EU model clauses) is in place for transfers of personal data outside the EU.	✓	
Art. 47	Failure to ensure that a competent supervisory authority approves Binding Corporate Rules (BCR); a failure to enforce the rights on data subjects with regard to the processing of their personal data within a group of com panies' subject to BCR, or a failure to follow the conditions for BCR outlined in Art.47 (e.g. data protection training for personnel with access to personal data).	✓	
Art. 48	Transfer of data following a court or tribunal order to a third country without an international agreement, such as a mutual legal assistance treaty being in place.	✓	

Vaimo AB | Tel: +46 8 452 26 50 | Rosenlundsgatan 40, 11853 Stockholm

PROCESSOR (VAIMO) OBLIGATIONS

ARTICLE	DESCRIPTION	LOW FINES	HIGH FINES
Art. 9	Processing of special categories of personal data (e.g. health data) when none the conditions in Art.9 have been met (e.g. explicit consent by the data subject).		✓
Art. 27	Failure to designate in writing a representative in the European Union for controllers or processors not established in the Union.	✓	
Art. 28	Failure by a controller to use a processor which provides sufficient guarantees to implement appropriate technical and organisational measures to ensure the protection of the rights of the data subject. Failure to put in place controller - processor obligations (e.g. contract in writing, restrictions on subcontracting).	✓	
Art. 29	Processing data without the express permission of the controller or processor.	✓	
Art. 30	Failure to maintain a detailed record of processing activities under a controller or processor responsibility (e.g. categories of data, purpose of processing, details of external transfers).	✓	
Art. 31	Failure to cooperate with the data protection supervisory authority.	✓	
Art. 32	Failure to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (e.g. encryption, pseudonymisation, business continuity).	✓	
Art. 33	Failure to notify supervisory authority of data breaches within 72 hours or provide a satisfactory reason for the delay.	✓	

Vaimo AB | Tel: +46 8 452 26 50 | Rosenlundsgatan 40, 11853 Stockholm

ARTICLE	DESCRIPTION	LOW FINES	HIGH FINES
Art. 33	Failure to notify supervisory authority of data breaches within 72 hours or provide a satisfactory reason for the delay.	✓	
Art. 37-39	Failure to appoint an independent and fully supported data protection officer.	✓	
Art. 41	Failure to take appropriate action in cases of infringement of approved GDPR codes of conduct.	✓	
Art. 42	Failure to adhere to Art.42 requirements relating to the implementation of data protection certification mechanisms or data protection seals and marks.	✓	
Art. 44	Failure to adhere to one or more conditions in Chapter V relating to transfers of Personal Data to Third Countries (e.g. outside the European Economic Union) or International Organisations.		✓
Art. 45	Transfers of personal data outside the EU to a country which the Commission has decided does not have an adequate level of protection.		✓
Art. 46	Failure to ensure legal mechanism (e.g. EU model clauses) is in place for transfers of personal data outside the EU.		✓
Art. 47	Failure to ensure that a competent supervisory authority approves Binding Corporate Rules (BCR); a failure to enforce the rights on data subjects with regard to the processing of their personal data within a group of companies' subject to BCR, or a failure to follow the conditions for BCR outlined in Art.47 (e.g. data protection training for personnel with access to personal data).		✓
Art. 48	Transfer of data following a court or tribunal order to a third country without an international agreement, such as a mutual legal assistance treaty being in place.		✓

Vaimo AB | Tel: +46 8 452 26 50 | Rosenlundsgatan 40, 11853 Stockholm