DATATILSYNET

10 September 2021

Serious criticism of Helsingør Municipality in Chromebook case

The Danish Data Protection Agency has ruled on the first in a series of cases concerning the use of Google Chromebooks and G Suite for Education (now called Workspace) in primary and lower secondary schools.

Summary

The Danish Data Protection Agency's decision in this specific case concerning the use of Google Chromebooks in Helsingør Municipality states that the Primary and Lower Secondary Education Act gives local authorities the right to choose the IT equipment and software to be used in teaching.

It is the responsibility of the local authority, as the controller, to ensure that the IT equipment and software are used in such a way that data protection rules are complied with. In particular, the processing carried out must not go beyond the purpose prescribed by the Primary and Lower Secondary Education Act. The Danish Data Protection Agency cites the disclosure of personal data for marketing or profiling purposes as an example of processing that falls outside the purposes prescribed by the Primary and Lower Secondary Education Act.

In this specific case, the local authority had not carried out the necessary assessments of the risk to the rights of data subjects.

In its decision, the Danish Data Protection Agency states that, for certain aspects of setting up Chromebooks and using G Suite, it is necessary to configure access to the applications and the way they function in order for them to be used lawfully.

As the local authority had not assessed this, it also had no documentation to show that the configuration had been carried out in a manner appropriate to the risks to data subjects.

The Danish Data Protection Agency found that the lack of assessments led to several breaches of the Regulation.

The Danish Data Protection Agency issued an order to Helsingør Municipality to bring its processing of data into compliance with the Regulation. If the municipality was unable to mitigate the risks associated with the processing, it would be subject to a restriction preventing it from processing the data in question after a specified deadline.

In addition, the Authority expressed serious criticism of the municipality's data processing practices. The Authority also issued a warning to Helsingør Municipality that the use of add-on products for G Suite could not be processed lawfully without a data protection impact assessment having been carried out, in which the risks associated with the processing had been reduced to less than a high risk to the rights and freedoms of data subjects.

Decision

The Danish Data Protection Agency hereby returns to the case in which Helsingør Municipality reported a personal data breach to the Danish Data Protection Agency on 29 January 2020.

In light of several relatively similar breaches by other controllers, parts of the investigation have been conducted jointly and in parallel across these cases.

1. Decision

Following a review of the case, the Danish Data Protection Agency finds that there are grounds for issuing an **order** to Helsingør Municipality to bring the processing operations involving the use of Chromebooks into compliance with the Regulation, cf. Article 58(2)(d) of the General Data Protection Regulation. This is to be achieved by Helsingør Municipality undertaking the following **by 1 November 2021**: A risk assessment of the processing operations involving Chromebooks and G Suite, reflecting the flows of personal data involved in such processing. The risk assessment must address both the necessary options for configuring the product and the scope of the legal basis provided by the Primary and Lower Secondary Education Act in relation to the use required of pupils. Should the risk to data subjects and their fundamental rights be assessed as high, the order also requires the preparation of an impact assessment.

The Danish Data Protection Agency is issuing a **warning** to Helsingør Municipality that the use of G-Suite add-on programmes without carrying out a data protection impact assessment will be in breach of the General Data Protection Regulation, unless the assessment now required by this order demonstrates that the risk to the rights and freedoms of data subjects is not high. The warning is issued pursuant to Article 58(2)(a) of the General Data Protection Regulation.

Should the risk assessments carried out by Helsingør Municipality indicate a high risk to the rights and freedoms of data subjects, and should these risks not be reduced to a level lower than high before the deadline for compliance expires on 1 November 2021, the Danish Data Protection Agency hereby imposes on Helsingør Municipality **a temporary limitation on processing**, such that processing involving a high risk to the rights and freedoms of data subjects may not take place after that date, until such time as the risk has been reduced to a level lower than high. The restriction on processing is imposed pursuant to Article 58(2)(f) of the General Data Protection Regulation.

Failure to comply with an order or a temporary limitation may, unless a more severe penalty is applicable, be punishable by a fine or imprisonment for up to six months, cf. Section 41(2), no. 4 of the Data Protection Act.

With regard to the infringements identified, the Danish Data Protection Agency, in addition to the corrective measures already adopted, expresses **serious criticism** of the fact that Helsingør Municipality's processing of personal data has not been in accordance with Article 5(2) of the General Data Protection Regulation:

Article 5(2), cf. Article 5(1)(c) and (f),

Article 5(1)(a), in conjunction with Article 6(1),

Article 32(1), Article 33(1) and Article 35(1).

Below is a detailed review of the case and the grounds for the Danish Data Protection Agency's decision.

2. Statement of the case

On 29 January 2020, Helsingør Municipality reported a personal data breach to the Danish Data Protection Agency.

It is apparent from the report and subsequent detailed statements that Helsingør Municipality has issued Google Chromebooks to the municipality's school pupils for use in teaching at the municipality's primary and lower secondary schools. In connection with the issue of these devices, the municipality set up access to Google G Suite for Education (hereinafter 'G Suite'), for which a Google account is required. The pupil's full name was used for this school account and was thus accessible to other products of Google Inc. (hereinafter 'Google'), to which the school accounts created were disclosed by Google – including the YouTube platform – a fact of which Helsingør Municipality was unaware, nor was this the intention. It further emerges from the case that pupils – provided they used the YouTube platform – were automatically granted access via their school account and had their full names displayed in connection with their posts on this platform, unless the municipality had assigned them anonymised usernames.

It is apparent from the case that Google – reportedly since 2015 – has offered a software package called G Suite. The software package is specifically aimed at the education of children and young people and is therefore considered suitable for use in teaching. The programmes can be supplied by a number of companies as a package solution, which may include a laptop, the software suite, installation and set-up, as well as specially developed teaching materials. In order for pupils to access the programmes in G Suite, they must have a school account set up with Google. The account can be created manually, but it is also possible to create school accounts by transferring first names, surnames, school and year group from the schools' administrative systems, provided that pupils with protected name and address details can be anonymised by assigning them an alias instead of their real name. Despite this, there have been several instances where pupils' full names have been listed instead of aliases.

Helsingør Municipality has – like a large number of other municipalities in the country – procured and distributed laptops with the software package pre-installed, acting within the scope of their official powers under the Danish Primary and Lower Secondary School Act; consequently, they did not consider it necessary to obtain parental consent for the creation of pupils' school accounts with Google.

In 2019, Google amended the terms of service for G Suite so that a number of additional products were covered by the agreement. These products included YouTube, Gmail, Blogger, Google+, etc., and Google states that the terms of service apply to all services provided by Google and its affiliated companies, including YouTube.

Google's terms and conditions governing the use of G Suite state that access to the system for children under the age of 13 requires parental consent, and that for young people under

the age of 18, access to additional services, including YouTube, also requires parental consent.

G Suite has a user administration module that allows you to select which systems and add-on services pupils should have access to. It is therefore possible, through active intervention, to block pupils' access to, for example, YouTube, Gmail, etc.

Pupils in Helsingør Municipality have been granted access to the add-on services via their school accounts, thereby enabling them to post content and comment on others' posts on platforms such as YouTube. When using these services, details such as the pupil's name, school and class – as provided when the account was created – will be displayed alongside the post.

The Danish Data Protection Agency has received two complaints concerning Helsingør Municipality's processing of personal data in connection with the distribution of Chromebooks. Both complaints state that Helsingør Municipality, without the parents' knowledge or consent, created Google accounts for the pupils, thereby giving them access to a range of Google programmes under G Suite, including Gmail and the add-on YouTube. The complaints further state that the pupils' full names are displayed when using Gmail and that parents are unable to correct or anonymise this information, as only Helsingør Municipality has access to the user administration panel.

It is also stated that pupils' full names, schools and year groups appear on YouTube if the pupil has created or commented on a post.

The complainants also point out that the computers issued to pupils have their login details stuck on them, meaning that there is effectively no protection against unauthorised access to the pupils' accounts.

3. Information from Helsingør Municipality

In its response to the Danish Data Protection Agency, Helsingør Municipality has stated that the municipality has entered into an agreement with Google as a processor regarding the use of Chromebooks and the creation of school accounts containing the pupils' names, schools and year groups. The school profiles have been created in accordance with the schools' exercise of authority under the Danish Primary and Lower Secondary School Act, under which they are legally obliged to provide IT education. For this reason, the municipality has not sought parents' consent to the creation of accounts for the pupils. The local authority has further stated that, for a G Suite school profile, the pupil owns all the data.

When creating pupils' school accounts, data is retrieved from the school administration system; however, in the case of protected personal data, a procedure is followed whereby an alias is assigned instead of the pupil's full name. However, Helsingør Municipality has stated that, on several occasions, the municipality has entered a pupil's full protected name instead of an alias, thereby creating a risk that the protected name could be disclosed.

Following changes to Google's terms and conditions for the use of G Suite, a number of add-on programmes, including YouTube, were made available to school pupils via their school accounts. Helsingør Municipality was not aware of this.

In its consultation response of 6 January 2020, Helsingør Municipality confirmed that, in 2019, a parent complained that his child – without his knowledge – had had a YouTube account created, meaning that the child's name could be made public on YouTube.

As it was not the intention that pupils should use programmes other than the core programmes in G Suite, Helsingør Municipality was not aware that the use of additional programmes could result in the publication of pupils' names on platforms such as YouTube. For the same reason, Helsingør Municipality did not carry out a risk assessment, including for loss of confidentiality, in relation to the processing in question. Similarly, Helsingør Municipality did not implement technical or organisational measures to safeguard the rights of data subjects in connection with the use of social media via the school account that had been created.

Helsingør Municipality has blocked access to YouTube via G Suite, thereby ensuring that, going forward, pupils will not be able to publish information about themselves. However, the municipality states that it is the responsibility of the pupil's parents to delete the pupil's profile and any unwanted content on social media, as this cannot be done via the municipality's user administration panel. The municipality has stated that it has amended the publicly available information to include only the first name and school.

Helsingør Municipality has assessed that it was unlikely that the incident could pose a risk to the rights and freedoms of data subjects and has therefore not deemed it necessary to notify the Danish Data Protection Agency. Helsingør Municipality has taken the view that the information inadvertently shared with YouTube consists of ordinary personal data in the form of names, school and year group – information which, in the municipality's opinion, does not in itself make it possible to contact the individual directly or to collect information about their behaviour. Furthermore, Helsingør Municipality has taken the view that YouTube is owned by Google and that Google has not been granted access to any information beyond that already provided for under the original G Suite agreement. The municipality has further taken the view that the information in question is general in nature, and that it is unlikely that this information, in itself, could be misused for purposes such as identity theft.

On 21 January 2020, Helsingør Municipality informed all parents of the incident and has drawn greater attention to the settings available in the G Suite user administration console.

4. Reasons for the Danish Data Protection Agency's decision

4.1 General

It follows from section 2(1) of the Primary and Lower Secondary Education Act that the local council is responsible for primary and lower secondary schools.

Furthermore, for primary schools, it follows from sections 18(1) and 19 of the same Act that this includes the organisation of teaching, including the choice of teaching and working methods, approaches, teaching materials and subject selection, as well as the funding thereof.

It is the Danish Data Protection Agency's view that both decisions regarding the use of IT in teaching and the choice of hardware and software to be used fall within this scope of discretion.

Data protection rules are technology-neutral, and the Danish Data Protection Agency can only assess the circumstances arising from the processing of personal data carried out, cf. Article 2(1) of the General Data Protection Regulation.

This decision therefore relates solely to the processing of personal data carried out on the chosen hardware and software, and whether this takes place within the framework prescribed by the General Data Protection Regulation and the Data Protection Act.

4.2 The use of Chromebooks and G Suite

The rights of children and young people enjoy special protection under data protection rules. It is the Danish Data Protection Agency's view that this consideration forms part of the assessment of which processing operations may be carried out on the basis of the legal authority granted to individual local authorities by the Primary and Lower Secondary Education Act.

Based on the information provided to the Authority regarding this case, and following a review of the submitted material, the data processing agreement with Google, as well as a review of the configuration options when creating users and configuring settings within the applications, it is the Danish Data Protection Agency's view that Helsingør Municipality would have been able to issue Chromebooks and implement G Suite (the original core programmes) for educational purposes, and process the required information on the basis of Article 6(1)(e) of the General Data Protection Regulation; this also applies to the creation of individual pupils as users of the system.

In making this assessment, the Danish Data Protection Agency has placed particular emphasis on the fact that both the use of a Chromebook, the initial registration of pupils in the system and the use of the part of G Suite that constitutes the basic package can be configured in such a way that no processing takes place that exceeds the scope of the municipality's authority within the framework of its exercise of public authority, in accordance with the provisions of the Primary and Lower Secondary School Act concerning the purpose of primary and lower secondary schools and the provision of teaching resources. The Danish Data Protection Agency has taken as its basis that it is evident from the data processing agreement and the configuration options for the individual units that data, including personal data, can be managed in such a way that it is not processed outside the EU/EEA; that information about individual users can be minimised to an alias; and that data, including personal data, generated through the use of the applications in G-Suite (the core programmes) can be configured so that only the individual data subject and administrators authorised by the local authority will be able to access this data; in particular, that the information will not be used for marketing purposes, either directly, targeting the individual data subject, or indirectly as part of a group (class, year group, school, etc.).

It is the Danish Data Protection Agency's assessment that this configuration, particularly in relation to some of the applications, will require parts of the functionality to be disabled. Furthermore, it is the Danish Data Protection Agency's assessment that, when using the product without this configuration, and during normal and expected use of the equipment, personal data may be transferred to services outside the EU/EEA. Such transfers will require compliance with the rules set out in Chapter 5 of the General Data Protection Regulation.

It is a prerequisite that, before the system is put into operation, certain documented decisions have been made which, on the one hand, ensure compliance with the principles set out in Article 5(1) of the General Data Protection Regulation – in this case, particularly points (c) and (f) – and, on the other hand, ensure that an assessment has been carried out as to whether a data protection impact assessment is required under Article 35 of the General Data Protection Regulation. This assessment must also be used to determine the necessary level of security in accordance with Article 32 of the General Data Protection Regulation.

The Danish Data Protection Agency assumes – in accordance with Helsingør Municipality's own explanation on this matter – that the municipality has not carried out a separate assessment of the risks to pupils' rights and freedoms arising from the processing of their personal data, the use of the purchased Chromebooks, the registration of pupils as users of these devices, and the use of the programmes in G Suite and the add-on programmes.

The Danish Data Protection Agency further finds that the local authority has not carried out an identification, evaluation and/or testing of configurations, and the resulting personal data flows arising from the use of the Chromebooks and G Suite applications in question, which were made available to pupils.

The Danish Data Protection Agency notes that the lack of documentation regarding the considerations of risks to the rights of data subjects and the assessments of the processing operations carried out means that Helsingør Municipality has been unable to demonstrate compliance with Article 5(1) of the General Data Protection Regulation, in so far as it concerns which personal data were necessary for user registration. In this regard, the Danish Data Protection Agency has placed particular emphasis on the fact that the municipality itself subsequently established that it was possible to minimise the information whilst still fulfilling the purposes of the processing. Furthermore, Helsingør Municipality has been unable to demonstrate compliance with Article 5(1)(f) of the General Data Protection Regulation. In this regard, the Danish Data Protection Agency has placed particular emphasis on the fact that the municipality was unable to demonstrate, what configuration was in place at the time of commissioning and thus unable to demonstrate that, at that time, adequate security had been ensured for the processing operations carried out.

Against this background, the Danish Data Protection Agency finds that Helsingør Municipality has infringed Article 5(2) of the General Data Protection Regulation, cf. Article 5(1)(c) and (f).

4.3 G-Suites add-on products

It is the Danish Data Protection Agency's view that the legal basis for processing under the Primary and Lower Secondary Education Act cannot cover situations where personal data is used for purposes other than those necessary to fulfil the objectives of the Act, nor can it be lawfully disclosed to other controllers for their own purposes. This also means that pupils' use of the equipment and programmes must not generate personally identifiable information, including metadata, which is used for marketing and profiling; in particular, the information must not be used for marketing, either directly, targeting individual pupils, or indirectly as part of a group (class, year group, school, etc.).

In accordance with the information provided by Helsingør Municipality, the Danish Data Protection Agency assumes that the processing of personal data has taken place in G Suite's add-on products, with the consequent risk of unintentional disclosure of pupils' personal data, as well as the possibility of personal data being disclosed to a third party – without this being the municipality's intention – specifically authorised by the pupils' parents.

The Danish Data Protection Agency finds that such disclosure cannot be regarded as necessary for the municipality's exercise of its public authority. The processing that has taken place in G Suite's add-on products, and which has resulted in the disclosure of personal data to Google, has therefore lacked the necessary legal basis for processing.

On this basis, the Danish Data Protection Agency finds that Helsingør Municipality has infringed Article 5(1)(a) of the General Data Protection Regulation, read in conjunction with Article 6(1).

4.4 Risk and consequences

The Danish Data Protection Agency finds that Helsingør Municipality has not analysed the risks the changes to Google's terms of service might pose to school pupils if they used G Suite and its associated products, including YouTube.

It is the Danish Data Protection Agency's view that the use of new, complex technology, including software, particularly in the field of education where the data subjects are children and young people, generally falls within the area where the Agency assesses that it normally entails a high risk to the rights and freedoms of these pupils. In this specific case, where it is common knowledge that, in the choice of Chromebooks and the technologies used to provide system support, part of the business model for other parts of Google's products involves data collection, targeted marketing and the sale of this information, these factors must be taken into account in the assessment of the risks in question.

In view of this, it is the Danish Data Protection Agency's view that, in this specific case, there has been a high risk to the rights and freedoms of data subjects. The conditions for carrying out a data protection impact assessment, as set out in Article 35 of the General Data Protection Regulation, are therefore met.

By failing to carry out such an assessment, Helsingør Municipality has contravened Article 35(1) of the Data Protection Act.

It is the Danish Data Protection Agency's view that a specific risk assessment and impact assessment – prior to the provision of IT equipment to pupils and the processing of pupils' data – are essential for determining which security measures are necessary to achieve a level of security commensurate with these risks, and what consequences the processing of pupils' personal data may have for the individuals concerned. The Danish Data Protection Agency must point out that several of the infringements mentioned above could have been avoided had an assessment of the risks associated with the processing been carried out, followed by action based on those findings.

4.5 Personal data breaches and security of processing

The Danish Data Protection Agency bases its assessment – on the basis of Helsingør Municipality's own explanation – on the fact that there have been several instances where Helsingør Municipality has used pupils protected full names instead of an alias, which is otherwise the municipality's standard procedure. This created a risk that the pupils' full names – had the pupils in question used the social media platforms to which they had access via their school accounts – would have been published on those platforms; the Authority therefore finds that a personal data breach has occurred, cf. Article 4(12) of the General Data Protection Regulation.

4.6 Article 32 of the General Data Protection Regulation

It follows from Article 32(1) of the General Data Protection Regulation that the controller must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks associated with the controller's processing of personal data.

The Danish Data Protection Agency finds that Helsingør Municipality – in some cases – has provided pupils' computers with the pupil's login– meaning that anyone gaining access to the computer could log in and access the pupil's other data and personal data, just as it would be possible, for example, to post or tag content on YouTube or other media in the pupil's name. Such a procedure typically results in the note not being removed and the login details therefore not being kept confidential.

It further follows from Article 32 that the controller must implement appropriate technical and organisational measures to ensure, amongst other things, the ongoing confidentiality and integrity of processing systems and services, which, in the opinion of the Danish Data Protection Agency, has not been fulfilled, as the controller has provided computers issued to school pupils with visible login details.

The controller has a duty to identify the risks that its processing poses to data subjects and to ensure that appropriate security measures are put in place to protect data subjects against these risks.

It is the Danish Data Protection Agency's view that the requirement under Article 32 regarding appropriate security will normally mean that, in systems containing a large amount of confidential information about a large number of users, higher standards of care must be required of the controller in cases where personal data is disclosed, including ensuring that there is no unauthorised disclosure of personal data requiring special protection or sensitive personal data.

Furthermore, it is the Danish Data Protection Agency's view that all likely error scenarios should be tested when new programmes that process personal data are put into use.

In light of the above, the Danish Data Protection Agency finds that Helsingør Municipality – by **failing to** carry out a risk analysis to identify the risks that access to G Suite add-on products would entail for pupils, and by failing to analyse the potential consequences of school pupils gaining access to G Suite add-on products, including YouTube; **by failing to** carry out sufficient testing of the scope and functionality of G Suite's add-on products prior to their implementation; **by failing to** ensure that the names of pupils subject to name and address protection were anonymised; and **by failing to** implement adequate safeguards against unauthorised use of the computers issued to school pupils – has failed to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks associated with Helsingør Municipality's processing of personal data, cf. Article 32(1) of the General Data Protection Regulation.

- **reporting of the breach.**

The Danish Data Protection Agency further finds that Helsingør Municipality's assessment that no notification was required under Article 33 of the Data Protection Act, as it was unlikely that the personal data breach could pose a risk to the rights or freedoms of natural persons, is clearly not based on the facts of the case. In this regard, the Danish Data Protection Agency has emphasised that there were several breaches, a number of which resulted in an actual risk. Helsingør Municipality should therefore have notified the Danish Data Protection Agency of the personal data breach within 72 hours of becoming aware of it.

In doing so, Helsingør Municipality has failed to comply with the requirements of Article 33(1) of the General Data Protection Regulation.

4.8 Summary

In determining its response, the Danish Data Protection Agency has prioritised ensuring, as a matter of urgency, that Helsingør Municipality's processing activities are brought into compliance with the General Data Protection Regulation.

The Danish Data Protection Agency therefore issues an **order** to Helsingør Municipality to bring the processing operations involving the use of Chromebooks into compliance with the Regulation, cf. Article 58(2)(d) of the General Data Protection Regulation. This must be achieved by Helsingør Municipality carrying out the following **by 1 November 2021**: A risk assessment of the processing operations involving Chromebooks and G Suite, reflecting the flows of personal data involved in such processing. The risk assessment must address both the necessary options for configuring the product and the scope of the legal basis provided by the Primary and Lower Secondary Education Act in relation to the use required of pupils. If the risk to data subjects and their fundamental rights is assessed as high, the order shall also require the preparation of an impact assessment.

The Danish Data Protection Agency issues a **warning** to Helsingør Municipality that the use of G-Suite add-on programmes without carrying out a data protection impact assessment will be in breach of the General Data Protection Regulation, unless it is demonstrated by the assessment now required under the order that the risk to the rights and freedoms of data subjects is not high. The warning is issued pursuant to Article 58(2)(a) of the General Data Protection Regulation.

The Danish Data Protection Agency has noted that Helsingør Municipality has blocked pupils' access via school accounts to G Suite add-on applications, including YouTube.

Should the risk assessments carried out by Helsingør Municipality indicate a high risk to the rights and freedoms of data subjects, and should these risks not be reduced to a level lower than high before the deadline for compliance expires on 1 November 2021, the Danish Data Protection Agency hereby notifies that Helsingør Municipality **is subject to a temporary limitation on processing**, such that processing involving a high risk may not take place after this date until the risk has been reduced to a level lower than high. The limitation on processing is imposed pursuant to Article 58(2)(f) of the General Data Protection Regulation.

Failure to comply with an order or a temporary limitation may, unless a more severe penalty is applicable, be punishable by a fine or imprisonment for up to six months, cf. Section 41(2), no. 4 of the Data Protection Act.

With regard to the infringements identified, the Danish Data Protection Agency, in addition to the corrective measures already adopted, expresses serious criticism of the fact that Helsingør Municipality's processing of personal data has not been in accordance with Article 5(2) of the General Data Protection Regulation:

Article 5(2), cf. Article 5(1)(c) and (f),

Article 5(1)(a), in conjunction with Article 6(1),

Article 32(1), Article 33(1) and Article 35(1).

5. Concluding remarks

The Danish Data Protection Agency notes that it is the responsibility of Helsingør Municipality to rectify and erase data in accordance with this decision. The municipality must therefore contact the parents of the data subjects concerned in order to carry out the rectifications, anonymisations or erasures of the personal data that the parents cannot themselves carry out in the systems where the pupils' personal data have been inadvertently published or disclosed.

The Danish Data Protection Agency notes that its decision cannot be referred to any other administrative authority, cf. section 30 of the Data Protection Act.

However, the Danish Data Protection Agency's decision may be brought before the courts, cf. Section 63 of the Constitution.

The Danish Data Protection Agency hereby considers the case closed and will take no further action in this matter.

Annex: Legal basis

Extract from Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Article 2(1):

This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

Article 4:

For the purposes of this Regulation, the following definitions shall apply:

- 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

- 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

[…]

- 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the

processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

[…]

- 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Article 30:

Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
b) the purposes of the processing;
c) a description of the categories of data subjects and of the categories of personal data;
d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
e) 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;
f) where possible, the envisaged time limits for erasure of the different categories of data;
g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

Article 32:

1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

    a) the pseudonymisation and encryption of personal data;
    b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
    c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
    d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.
4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Article 33:

In the case of a personal data breach, the controller 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 competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

1. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
2. The notification referred to in paragraph 1 shall at least:

    a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
    b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
    c) describe the likely consequences of the personal data breach;
    d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

3. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
4. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34:

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).
3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.