CONTROLLER
Kry International AB

Swedish ref.:
IMY-2022-3822

IMI case register:
649079
Date:
2024-12-19

Final decision under the General Data Protection Regulation – Kry International AB

Decision of the Swedish Authority for Privacy Protection

The Swedish Authority for Privacy Protection (IMY) finds that Kry International AB (Kry), 556967-0820, has processed personal data in breach of Article 32(1) of the General Data Protection Regulation (GDPR)[1] by not implementing appropriate technical and organisational measures to ensure an appropriate level of security for personal data when using the Meta Pixel during the period May, 28 2020–May 17, 2022.

IMY issues a reprimand to Kry pursuant to Article 58(2)(b) of the GDPR for the infringement.

Presentation of the supervisory case

Background, etc.

On May 18, 2022 Kry notified IMY of a personal data breach. In the notification was inter alia stated that Kry had offered a service used for businesses to businesses in order to facilitate remote contact through a secure and encrypted video connection (the service). The users have typically been healthcare businesses (users) who have been able to register an account and then invite other organisations, colleagues, customers, patients and people representing patients (end-users) by sending out a link to a video meeting by for example text message and email. By using Meta Platforms Ireland Limited's (Meta's) analysis tool the Meta Pixel on the websites where the service was offered, hashed contact information about end-users has been unintentionally transferred to Meta. The incident was discovered by information from a third party.

IMY has initiated supervision in May 2022 in light of the information stated in the notification of personal data breach. The investigation has been limited to the question of whether Kry has implemented appropriate technical and organisational measures in

[1] 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).

Postal address:
Box 8114
104 20 Stockholm
Sweden
Website:
www.imy.se
E-mail:
imy@imy.se
Telephone:
+46 (8) 657 61 00

accordance with Article 32 of the GDPR with regard to the processing of the end-users' personal data.

Due to the cross-border nature of the supervisory case, IMY has made use of the cooperation and consistency mechanisms provided for in Chapter VII of the GDPR. The concerned supervisory authorities have been the data protection authorities in Denmark, Finland, France, Luxembourg, Netherlands, Norway, Poland, Germany, Hungary and Austria.

Kry's statements

Kry has essentially stated the following with regard to the matter examined in the case.

Controller
Kry is the data controller for the unintentional collection and sharing of end-users' personal data. The implementation of the Meta-pixel has been done by Kry in order to market Kry's own services. Kry has thus determined the purpose and means of the processing in question.

Purpose of the processing
Kry has used the Meta pixel for marketing purposes. The intention has been to collect a limited amount of data about website visitors and users in order to target ads, on Meta's social platform Facebook, to those visitors who have not yet registered an account or users who have registered an account without starting to use the service. The aim was also to evaluate the need and measure the effectiveness of such marketing. Kry has not intended to collect information about or target marketing to end-users. However, due to the activation of the Meta Pixels Automatic Advanced Matching function (AAM function), contact information provided by users about end-users to send out a video meeting invitation has been collected and transferred to Meta. The transmission of the data started on May, 28 2020 and ended on May, 17 2022.

The personal data that has been transferred to Meta
The personal data transferred about the users has included technical information about the users' device, IP address, hashed contact information in the form of email address and phone number, and interaction data such as button presses and events (for example, registration of account, opening of pages or creation of meeting links). The transmission of end-users' contact details has included either their email addresses or telephone numbers. There has been no collection and transmission of data on end-users' use of the service, such as information that the person clicked on a meeting link, joined a meeting or ended a meeting.

It should be noted that several transmitted contact details most likely do not constitute personal data according to the GDPR because they consisted of common email addresses such as info@caretaker.se or switchboard numbers. A review of the pilot project for the service and user feedback further shows that the service was used by healthcare providers inviting a legal entity, such as a health centre or accommodation, as an end-user to the video meeting. In such cases, the contact with the patient has taken place through the legal entity's unit and the booking has not included the processing of the patient's personal data.

The data on end-users did not include special categories of personal data pursuant to Article 9 of the GDPR, inter alia, for the following reasons. It has not been possible to

link data about the end-user to events or actions taken by the user of the service such as invitations or meetings. Meta is very unlikely to have been able to distinguish that the data transferred about the user and the end-user belonged to different parties, since no data suggesting who the data transferred related to was transferred. Activation of the AAM function has resulted in the end-user's email address or phone number being associated with the event instead of the user's email address and phone number. For Meta, it has thus looked like the user changed their contact information. Furthermore, according to the processing agreement that applies between Kry and Meta, Meta has only been allowed to match the contact information with people with accounts on Meta's platforms. Meta has thus also not had the right to try to connect the hashed contact information. Even if Meta could have determined that the data concerned different parties, it has not been possible for Meta to conclude that it was neither a patient nor a caregiver. This would require far-reaching assumptions by Meta as there are many possible links between the different platform accounts other than a healthcare provider and a patient. In addition, the data transferred about users have been professional data and accounts on Meta's platforms are typically of a private nature. It is therefore unlikely that the hashed contact details of the users matched Metas data and Meta has not been able to translate the hashed email address to a readable address.

Scope of the incident
An important principle of the platform and the service has been to not collect, store or otherwise process personal data about end-users. The contact details of the end-users have therefore been deleted from Krys' system immediately after the invitation was sent. For this reason, there are no records or storage of data that can be used to calculate the exact number of unique end-users. Based on the number of calls implemented through the platform and internal statistics from Kry's other services, Kry estimates that approximately 90 000 end-users may have been affected. However, a large part of the contact information of these end-users is unlikely to constitute personal data, which means that the number of data subjects affected by the incident is lower than the reported number.

Krys' investigation also shows that Meta's personal data processing has been limited. The contact details have only, and for a very short period of time, been used to identify Meta’s platform users as potential recipients of targeted advertisements and have not been used in any other way. In Sweden, no marketing via Meta was carried out during the period of the incident or afterwards. When Kry became aware of the incident, the pixel was immediately removed from the websites where the service was offered and marketing through Meta was stopped in all markets.

Technial and organisational measures
Kry has taken a number of organisational and technical measures based on the specific risk identified with the processing of personal data within the framework of the service. At the time of the implementation of the service, Kry had internal policies and processes in place. Prior to the commissioning of the service, a risk analysis was carried out, which resulted in an data protection impact assessment. The impact assessment resulted, among other things, in the processing of end-users' personal data being limited to the contact details necessary to send out a meeting invitation. Through data protection by design, Kry has limited as far as possible the extent to which users were able to add data to the system at all. Furthermore, it has been decided that contact data to end-users and other data that needed to be handled in order to provide the service, such as video calls, technical data and metadata about video meetings, would only be processed in real time and thus not saved in Krys'

system. When the marketing department would implement the pixel on the web pages in question, it has not been deemed necessary to carry out another data protection impact assessment because the risks were considered low.

Krys' investigation shows that the technical team that implemented the Meta pixel has not fully understood some of its functionality. Kry has implemented a customer data platform to ensure control over what data that was collected on the websites where the service was offered and to be able to implement overall data protection settings for all tracking. Kry has made a number of settings in the customer data platform to protect personal data, including that no tracking would take place of the end-user page and that directly identified information would be hashed. The AAM function, which caused the unintended transmission, was turned off in the customer data platform for privacy reasons. The incident occurred because opposite settings were made in Meta's own developer tool that was given preference. Since the purpose of the Customer Data Platform is to instruct third-party cookies and pixels, Kry did not foresee that the pixel settings would take precedence over the settings of the Customer Data Platform and thus cause the transfer of personal data. A feature that hashed identified data has been enabled in the customer data platform that allowed the data to be automatically converted from plain text to hashed form. Meta has thus only been given access to hashed personal data. The lack of understanding of the consequences of activating the AAM function, combined with the fact that the technical settings made for the pixel were given precedence over the settings in the customer data platform, thus resulted in hashed contact information to end-users being transferred to Meta even though it was never intended.

Kry applies a principle of minimum privileges, which means that no user role is granted higher privileges than needed to perform its tasks. Only 3–4 people in the marketing department have been able to read and configure the tool for the Meta pixel. The marketing department has continuously and regularly evaluated the statistics regarding the data points and events that the company has decided to collect through the pixel. In addition, an external party has conducted penetration tests of the service on two different occasions. No follow-up of which personal data was collected through the pixel and sent to Meta was done because Kry configured the customer data platform to ensure a limited and secure processing of personal data. Among other things, Kry had taken steps to ensure that no directly identifying personal data from the event data would be shared with Meta. Furthermore, Kry had not understood that the AAM function had been activated and thereby circumvented the privacy settings in the customer data platform form. In May 2022, a more in-depth review of what data was collected and sent to Meta was carried out, which confirmed that some end-user data was mistakenly sent to Meta through the AAM function.

At the time of the incident, Kry has had a general data protection audit programme in place as well as annual internal controls in the field of data protection, based on the requirements of the GDPR and taking into account in particular the risks associated with data processing. However, the risk to the Meta pixel in the context of this programme has been assessed as relatively low, in particular as a result of the target group on which Kry intended to collect data and the measures taken to comply with the applicable legislation. Therefore, it was considered that there was no risk to the AAM function requiring further action as several appropriate measures had already been taken.

When the incident was detected, the Meta pixel was removed from the web pages where the service was offered. Kry has subsequently taken several measures in the

form of, among other things, investigating the incident and informing the data subjects about it on the websites where the service was offered. Kry has also contacted Meta and asked the company to delete the transferred data. Meta informed that all hashed data shared with Meta will be deleted within 48 hours. Kry has also taken steps to improve its handling of tracking technologies. Furthermore, other forward-looking measures have been taken in the form of, for example, reviewing existing requirements and guidelines, training measures and planning the review of functionality in the customer data platform. Kry has not sought or benefited financially from the unintended sharing of data.

Motivation for the decision

IMY will first consider whether the GDPR applies and whether IMY is the competent supervisory authority. If so, IMY will examine whether Kry is the data controller and whether it has implemented appropriate security measures under Article 32 of the GDPR to protect the personal data processed on end-users through the Meta pixel, with the AAM functionality enabled, during the period from May, 28 2020 to May, 17 2022.

IMY's competence

Applicable provisions
It follows from Article 95 of the GDPR that the GDPR shall not impose any additional obligations on natural or legal persons who process personal data, for those areas that are already subject to obligations under the so-called ePrivacy Directive. The ePrivacy Directive has been implemented into Swedish law by the Electronic Communications Act (2022:482) (LEK), which regulates, inter alia, the collection of data through cookies.

Pursuant to Chapter 9, Section 28 of LEK, which implements Article 5(3) of the ePrivacy Directive, data may be stored in or gained from a subscriber's or user's terminal equipment only if the subscriber or user has access to information about the purpose of the processing and consents to it. This does not prevent storage or access which is necessary for the transmission of an electronic message over an electronic communications network or which is necessary for the provision of a service expressly requested by the user or subscriber. The current LEK act entered into force on August, 22 2022. However, during the period in question in this supervisory case, the same requirements applied under Chapter 6, Section 18 of the Electronic Communications Act (2003:389). The Swedish Post and Telecom Authority (PTS) is the supervisory authority under LEK (Chapter 1, Section 5 of Ordinance [2022:511] on electronic communications).

The European Data Protection Board (EDPB) has issued an opinion on the interplay between the ePrivacy Directive and the GDPR. It follows, inter alia, from that opinion that the national supervisory authority designated under the ePrivacy Directive is solely competent to monitor compliance with that directive. However, according to the GDPR, IMY is the competent supervisory authority for the processing that is not specifically regulated in the ePrivacy Directive.[2]

[2] Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, paragraphs 68 and 69.

On October, 7 2024 the EDPB adopted guidelines on the technical scope of Article 5(3) of the the ePrivacy Directive. The guidelines states, among other things, that a common tool for companies is the use of unique identifiers or persistent identifiers. Such identifiers can be derived from persistent personal data (name, surname, email address, phone number, etc.), which is hashed on the user's device, collected and shared between several controllers to uniquely identify a person through different data sets (user data collected through the use of a website or application, customer relationship management relating to online or offline purchases or subscriptions, etc.). The Guidelines clarify that the fact that the information is entered by the user does not exclude the applicability of Article 5(3) of the the ePrivacy Directive, as the information is temporarily stored on the terminal before it is collected. In the case of collection through unique identifiers on web pages or mobile applications, the entity collecting is instructing the browser (through the distribution of client-code) to send that information. As such a gaining of access is taking place and Article 5(3) in the ePrivacy Directive applies.[3] The fact that the entity instructing the terminal to send back the information is not the same as the one receiving the information does not exclude the applicability of Article 5(3) of the the ePrivacy Directive.[4]

IMY's assessment
The supervisory case is about Krys' use of the Meta-pixel, a script-based tool in the form of a piece of code, on the websites where the service was obtained. The activation of the Meta Pixels AAM function has resulted in the pixel instructing the users' browsers to collect and hash information entered by the users on the website about themselves and the end-user. Based on this data, a unique identifier has been created that is temporarily stored in the user's terminal and then transferred to, and thus gained by, Meta for matching. The processing in question has thus included both storage in and gaining access from the user's terminal equipment referred to in Chapter 9, Section 28 LEK, and the corresponding provision in Chapter 6, Section 18 of the Electronic Communications Act (2003:389).

PTS is solely competent supervisory Authority of the application of the LEK. However, IMY's supervisory case concerns whether Kry has implemented sufficient security measures, which is not specifically regulated in the LEK. IMY is therefore competent to investigate the matter to which the supervisory case relates.

Controller of the processing

Applicable provisions
According to Article 4(7) of the GDPR, the controller is the person who, alone or jointly with others, determines the purposes and means of the processing of personal data. The fact that purposes and means can be determined by more than one actor means that several actors can be controllers for the same processing.

Pursuant to Article 5(2) of the GDPR, the controller must be responsible for and be able to demonstrate compliance with the principles set out in Article 5(1) (principle of accountability).

[3] Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, paragraphs 61–63.
[4] Ibid, paragraph 34.

IMY's assessment
Kry has stated that the company is the data controller for the processing of personal data that the use of the Meta pixel involved and for the transfer of personal data to Meta.

The investigation shows that Kry has decided to introduce the Meta pixel, a tool that tracks website visitors' actions and transmits the information to Meta, on the web pages where the service was offered and then activated the AAM function through the settings in Meta's tool. The purpose of the use of the Meta-pixel has been to promote Krys service and follow up on this marketing. Kry has therefore decided how the processing should be carried out and for what purpose the personal data should be processed. IMY therefore considers that Kry is the data controller for the processing of personal data that has taken place through the use of the Meta pixel with the AAM function enabled.

Has Kry ensured an appropriate level of security for the personal data?

Applicable provisions

Definition of personal data

According to Article 4(1) of the GDPR, personal data is any information relating to an identified or identifiable natural person. 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.

The requirement to implement appropriate security measures

It follows from Article 32(1) of the GDPR that the controller must take appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed by the processing. According to that provision, it must take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks, of varying likelihood and severity, to the rights and freedoms of natural persons. According to Article 32(1), appropriate safeguards include, where appropriate:

a) pseudonymisation and encryption of personal data;
b) the ability to ensure the 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 and
d) a process for regularly testing, examining and evaluating the effectiveness of technical and organisational measures to ensure the security of processing.

Recital 75 of the GDPR sets out factors to be taken into account when assessing the risk to the rights and freedoms of natural persons. It mentions, inter alia, the loss of confidentiality of personal data covered by the obligation of professional secrecy and whether the processing relates to data concerning health or sex life. Account shall also

be taken of whether the processing concerns personal data of vulnerable natural persons, in particular children, or whether the processing involves a large number of personal data and concerns a large number of data subjects.

Recital 76 of the GDPR states that the likelihood and seriousness of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. The risk should be evaluated on the basis of an objective assessment, which determines whether the data processing involves a risk or a high risk.

Data concerning health

Data concerning health belongs to the special categies of personal data, so-called sensitive personal data, which are given a particularly strong protection under the General Data Protection Regulation. As a general rule, the processing of such personal data is prohibited under Article 9(1) of the GDPR, unless the processing is covered by one of the exceptions in Article 9(2) of the GDPR.

Data relating to health are defined in Article 4(15) of the GDPR as personal data relating to the physical or mental health of a natural person which provide information on his or her health status. Recital 35 of the GDPR states that personal data concerning health should include all data relating to a data subject’s state of health which provide information on the data subject’s past, present or future physical or mental state of health.

IMY’s assessment

The process has involved a risk

The controller shall implement measures to ensure a level of protection appropriate with regards to the risks of the processing. The assessment of the appropriate level of protection shall take into account, inter alia, the nature, scope, context and purposes of the processing and the risks, of varying likelihood and severity, to the rights and freedoms of natural persons. On the basis of an objective assessment, it shall be determined whether the processing involves a risk or a high risk.

The investigation in the case shows that Kry has transferred data to Meta about the users of the service in form of, among other things, email address and information about how they acted, for example, in the form of registering an account, opening pages or creating meeting links. Furthermore, the contact details, in the form of email address or phone number, that the user entered about the end-user, in order to create an invitation for a meeting, have been transferred to Meta.

IMY makes the following assessment of the risks associated with the processing of the end-users' personal data.

The kind of data transferred to Meta in the present case may, at least as regards the personal email addresses and telephone numbers, constitutes data capable of directly or indirectly identifying a natural person and thus constitutes personal data. IMY also notes that it cannot be ruled out that it may have been possible to infer from the data transmitted that an invitation to a meeting between the user and the end-user has

been sent. Furthermore, in many cases, it must have been clear from the user's email address that he or she represented a healthcare provider.

However, the transfer in question did not include any information about the relationship between the user and the end-user or any information about what the booking was about. It has thus not been possible to deduce that the end-user was a patient, nor that the meeting constituted a health care visit or what health problems such a visit would concern. IMY therefore considers that the transferred data does not contain any information about the health status of the end-user and thus do not constitute sensitive personal data under the GDPR.

However, given that the service has been used in the healthcare business, IMY notes that the processing, although not involving sensitive personal data on health, has occurred in a context where data subjects must have been able to expect a high degree of confidentiality. This is especially true when the service was used for meetings between a healthcare provider and a patient. In addition, Kry has estimated that up to 90 000 end-users have been affected by the incident.

In conclusion, IMY considers that, having regard to its nature, scope and context, the processing has involved a risk that has required Kry to ensure a level of protection appropriate to the risk in question. Those measures were intended, inter alia, to ensure that personal data were protected against loss of control.

Kry has not implemented enough security measurements

IMY shall then assess whether Kry has ensured the level of protection required to protect the end-users' personal data.

Kry has stated that the company made settings in its Customer Data Platform to prevent the use of the Meta pixel's AAM function. However, the company's investigation shows that the function in question has nevertheless been activated because the opposite settings were made in Meta's tool for developers, which was given priority over the settings in the Customer Data Platform. The activation of the AAM feature has resulted in Kry unintentionally transferring end-users' contact information to Meta. However, Kry has taken security measures before the current processing which limited the negative consequences of the unintentional transfer. Among other things, Kry has decided to limit the processing of the end-users' data to what was needed to send out the meeting invitation and implemented technical barriers that prevented the user from entering more data than that. These restrictions have resulted in that it was not possible to read out what the current meeting invitation was about or any other privacy-sensitive information about the data subject.

IMY notes, however, that a basic prerequisite for Kry to be able to fulfill its obligations according to the data protection regulation is that the company is aware of what processing that is taking place under its responsibility. Kry has stated that the company has procedures in place to follow up its processing of personal data. According to the company, however, no follow-up was made of which personal data was collected and transferred to Meta through the pixel, because settings had been made in the customer data platform that would ensure a limited and secure processing of personal data.

For a long period, from May 28, 2020 to May 17, 2022 Kry transferred data about the end-users to Meta that was not intended to be transferred. Only after the company

received information about the incident from a third party did the company carry out investigations that confirmed that such a transfer had taken place. Against this background, IMY assesses that Kry cannot be considered to have had the systematic procedures required to identify such unintentional changes to the processing of personal data as the activation of the Meta-pixel's AAM function entailed. This has meant that Kry lacked control over the treatment and the ability to detect the current deficiency. IMY therefore assesses that Kry, even taking into account the security measures implemented at the time of the breach, cannot be considered to have implemented all the appropriate technical and organisational measures in relation to the risks that the processing has involved. Kry has therefore processed personal data in violation of Article 32 (1) of the GDPR.

Choice of corrective measure

IMY has corrective powers to use against controllers that has violated the GDPR. It follows from Article 58(2)(i) and Article 83(2) of the GDPR that the IMY has, inter alia, the power to impose administrative fines in accordance with Article 83 of that regulation. In the case of a minor infringement, IMY may, as stated in recital 148 of the GDPR issue a reprimand pursuant to Article 58(2)(b) instead of imposing an administrative fine. In the assessment IMY should consider aggravating and mitigating circumstances of the case, such as the nature, gravity and duration of the infringement and previous relevant infringements.

Kry has processed personal data with an insufficient level of security, which led to an unintentional transfer of personal data relating to a large number of data subjects to Meta. The transfer has been going on for a long time and has not been detected and corrected until a third party informed Kry of the deficiency. The infringement has occurred in a healthcare business where data subjects must be considered to have had a legitimate expectation of a high degree of confidentiality. However, Kry has impemented several measures that have limited the intrusion of the customers' privacy and, among other things, meant that the unintentional transfer did not include data of a privacy-sensitive nature. Furthermore, the measures taken by the company have led to the personal data being transferred in hashed, i.e. illegible, format to a single recipient and it is therefore not an uncontrolled disclosure where, for example, the data has been shared with many unauthorised persons or has been publicly available on the web.

On an overall assessment, IMY considers that this is a minor infringement as referred to in recital 148 of the GDPR and that Kry should therefore be given a reprimand.

This decision has been made by Head of Unit Nidia Nordenström after presentation by legal advisor Maja Welander. The IT- and Information Security Specialist Petter Flink has also participated during the processing of this case.

How to appeal

If you wish to appeal the decision, you should write to the Swedish Authority for Privacy Protection (IMY). Indicate in the letter which decision you wish to appeal and the change you are requesting. The appeal must have been received by IMY no later than three weeks from the day you received the decision. If the appeal has been

received in time, IMY will then forward it to the Administrative Court in Stockholm for review.

You can e-mail the appeal to IMY if it does not contain any privacy-sensitive personal data or information that may be covered by confidentiality. IMY's contact information is shown in the first page of the decision.