Warsaw, 08.06.2020

When does the processor become a controller?

Can the processor also act as a controller in the course of a personal data processing entrustment agreement? Can the processor, after termination of the entrustment agreement, become the controller of personal data which it previously processed only on behalf of another entity? Answers to these questions are important for determining the duties and potential responsibilities of the entities involved in the personal data processing.

By definition, the processor does not decide for itself on the purposes and means of the processing of personal data, but carries out processing operations only on instructions from and on behalf of the controller. In principle, a contract is the basis for the processing of personal data, which must specify in particular: subject, duration, nature and purpose of processing, type of personal data, categories of data subjects. The processor is authorised to process personal data only within the scope set out in the above agreement and the controller's instructions.

Change of role during the duration of the entrustment agreement

It may happen that in the course of the entrustment agreement the processor goes beyond the scope of processing specified in the agreement. In such a case, it will not act on the basis of an instruction from the controller - e.g. due to a change in the purpose or method of processing personal data designated by the ordering party. In such a situation, does the processor continue to act as a processor? It depends on the circumstances of the specific case, i.e. how far the processor will go beyond the controller's instructions and for what reason. It should be remembered that it is not the contract that determines the roles in the processing of personal data, but the factual situation.

A processor may go beyond the controller's instructions in order to ensure that the processing is as lawful as possible (if for some reason the framework set by the controller did not ensure such compliance). In this case, the processor should be considered to retain its original role. However, it may also be the case that the processor will use the personal data entrusted to it for its own purposes and decide on the means of processing itself. In such a case, if there is no legal basis for the processing of personal data of its own, it should be treated as a culpable breach of the entrustment agreement. The processor will act as a controller in this respect with all consequences. Therefore, it will be responsible for the lack of legal basis for the processing, lack of fulfilment of information obligations towards the data subjects, as well as for possible inadequate protection of the processed data.

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł

To perform a dual role legally

However, in the course of the entrustment agreement, is it possible for the processor at the same time to fulfil the role of the controller in accordance with the law in relation to personal data of the same scope as the data entrusted by another entity? In my opinion, yes. As an example I would indicate the relationship between the recruitment agency and its client - potential employer. On the one hand, the recruitment agency, when creating its database of candidates, obtains permissions to process the personal data of these persons in order to take them into account in future recruitment processes conducted for its clients. The scope of the processed personal data is the information contained in the CV. Moreover, the agency may process candidates' data for other purposes - e.g. name and surname and e-mail address will be used for marketing purposes (informing about various events organized by the agency, conducting surveys on the situation on the labour market and preparing reports on this basis, etc.). On the other hand, the recruitment agency, after providing the potential employer with the data of the selected candidate from its database, may be commissioned by the client to conduct additional services concerning this particular candidate, which are not normally included in the scope of recruitment services. This may involve negotiating an employment contract, providing the candidate on behalf of the client with information on the processing of personal data, or conducting a satisfaction survey of the employed person during the first period of employment. The agency will then process the candidate's identification data (and possibly other data), which it already has in its database, but the purposes and method of processing in the scope ordered by the client will be completely different from the purposes set by the recruitment agency for its own purposes. I believe that in this case, the recruitment agency will therefore, in accordance with the law, perform both the function of controller and the role of processor with regard to the same data (i.e. data with the same content) concerning the same person.

Further processing after termination or expiry of the entrustment contract

The contract of entrusting the processing of personal data is usually concluded for the duration of the main contract (service contracts). As a rule, upon termination or expiration of the contract, the processor should, depending on its provisions, return or delete the entrusted personal data. Then it stops participating in any way in the processing of personal data which it previously processed on behalf of the controller. However, does this always happen? Not necessarily.

First of all, the processor may not be able to return or delete the entrusted personal data soon (e.g. within 14 days) after the end of cooperation for technical reasons. It may also be that it is the controller who instructs the processor to continue to store the personal data, despite the termination of the main agreement. This will involve further performance of the role of the processor by the contractor (despite termination of the main service) until the period of deletion (or return) of personal data agreed by the parties. However, this should be explicitly regulated in the entrustment agreement.

Secondly, according to Article 28(3)(g) of the GDPR, upon termination of the provision of processing services, a processor is not obliged to return or delete personal data entrusted to him/her if Union law

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł

or Member State law requires the storage of personal data. In that case, the entity in question will continue to act as a processor, but on the basis of the relevant legal provisions and the processing will be limited to the storage of personal data only. In practice, however, it is difficult to find an example of such a regulation. In those cases where a specific entity provides services to the controller and is obliged to store personal data for the period specified in the regulations, the service provider is rather considered as a separate controller from the beginning (examples include insurance brokers or advocates and legal advisers).

Thirdly, in practice, I have encountered situations where processors want to process personal data entrusted to them after the termination of a contract for their own purposes, namely for purposes of proof. In entrustment agreements, there are provisions according to which the controller agrees that after the services are provided by the processor it will process the personal data received by the controller. The purpose of such processing is usually indicated as the necessity of proving the cooperation between the parties, defense against potential claims of the data subjects or the necessity of proving the processing of personal data in accordance with the law. Is such practice correct? What is the status of the original processor then? It should be emphasized that if such an entity processes entrusted personal data after the end of the service, in its own interest and exclusively for its own purposes, it will become an independent controller. As a consequence, it will be obliged to fulfil the information obligation towards the persons whose data it processes pursuant to Article 14 of the GDPR (due to the acquisition of personal data from a third party). He will also have to demonstrate that he has a legal basis for processing these data and duly safeguard them.

However, can and should the original controller agree to further processing of personal data by the service provider as controller? It should be remembered that in such a situation the original controller will make personal data available to a separate entity and must have a legal basis for this. This is because sharing is one of the forms of personal data processing. It could be argued that such a basis could be the legitimate interest of the former service provider. However, this ground for processing can be invoked when the processing of personal data is necessary to achieve the purpose of the entity, and in addition, when the interests of the third party will prevail over the interests or fundamental rights and freedoms of the data subject. Both the original controller and the recipient of the data (who is also likely to invoke his or her legitimate interest in processing the data made available to him or her) should carry out a balancing test to determine whether this condition may indeed apply. In my opinion, in most cases, the result of such a test will not allow the data to be made available by the original controller and processed by the former service provider. Why?

Well, personal data must always be processed in accordance with the basic principles set out in Article 5 of the GDPR. These include the principles of legality, fairness and transparency and minimisation. Personal data may only be processed if and to the extent necessary to achieve the objective pursued. Does the service provider really need to keep the personal data entrusted to it in order to prove that cooperation between the parties has been established and that the services have been properly provided? In my opinion, no. After all, the fact of establishing cooperation is documented by the

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł

service contract itself and the entrustment agreement, which will usually be kept further by both parties. Therefore, you will not need the personal data which were the subject of the entrustment to prove the above circumstances. If the former service provider would like to keep, for example, correspondence which would demonstrate the correct fulfilment of his obligations, he could anonymise the personal data contained in such correspondence. Another solution could be to sign a protocol on the termination of the contract, in which the recipient of the service confirms the correct performance of the contract by the service provider.

Does the service provider have to keep personal data in order to defend itself against data subjects' claims or to demonstrate that it has processed the data lawfully? If there is no dispute about the processing of the entrusted data during the contract period, I cannot find an example when further processing by the service provider would be necessary. This would simply not be adequate. I have the impression that many processors implement these provisions thoughtlessly without even asking themselves: why do we need personal data after the termination of the contract? Do we really need to process this data?

Conclusions

In conclusion, it may happen that both the current and the former processor will act as a controller |in relation to the data entrusted to it. This will require the fulfilment of all obligations imposed on controllers by the GDPR. The role of the controller does not depend on whether the entity is processing personal data in accordance with the law or whether it is acting in breach of the law, due for example, to the lack of a legal basis under Article 6 or Article 9 of the GDPR. Particular attention should, in my view, be paid to those cases where the data originally entrusted are to be made available by the original controller to the former service provider after the termination of the cooperation. It is then very important to verify carefully whether the former processor actually has to process personal data for the purpose it has set. In many cases, it may be that they do not need it at all. In such a situation, both the original controller may be held responsible for the unlawful disclosure of personal data, and the former processor may be held liable for the inadequate processing of personal data for the purposes it has set.

Agnieszka Rapcewicz, iSecure Sp. z o.o.

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł