Processing employee data under art. 6 paragraph 1 point f) GDPR

Przetwarzanie danych pracowniczych na podstawie art. 6 ust. 1 lit. f RODO

Arkadiusz Sobczyk
Professor Jagiellonian University, Poland

Summary Processing personal data in employment relations in Poland will be based primarily on the prerequisites laid down in art. 6 paragraph 1 GDPR *i.e.*: legal obligation, performance of public tasks and even protection of vital interests of a data subject. The above arises from the fact that labour law is highly codified. For this reason, processing personal data by the employer based on the legitimate public interest of the controller or of a third party will be rare. It may be that in the countries where rights and duties in an employment relationship arise primarily from collective agreements the situation is different. The subject of this text is to analyse what art. 6 para. 1 point f) GDPR offers in employment relations in the context of the interest of the employer.

Keywords: GDPR, personal data, work establishment, interests of a work establishment, interests of data controller, processing personal image.

Streszczenie Zdaniem autora przetwarzanie danych osobowych w stosunkach pracy w Polsce będzie się opierało w dominującym zakresie na zawartych w art. 6 ust. 1 RODO przesłankach obowiązku prawnego, wykonywania zadań publicznych, a nawet ochrony żywotnych interesów podmiotu danych osobowych. Wynika to z faktu, że prawo pracy w Polsce jest silnie skodyfikowane. Z tego powodu przetwarzanie danych osobowych przez pracodawcę w oparciu o uzasadniony interes administratora lub osoby trzeciej będzie rzadkością. W krajach, w których prawa i obowiązki w stosunkach pracy wynikają przede wszystkim z układów zbiorowych pracy, sytuacja wygląda inaczej. Przedmiotem artykułu jest analiza możliwości, jakie w relacjach pracowniczych daje art. 6 ust. 1 lit. f RODO, w szczególności w kontekście dobra zakładu pracy.

Słowa kluczowe: RODO, dane osobowe, zakład pracy, dobro zakładu pracy, interes administratora danych, przetwarzanie wizerunku..

Introductory notes

Protection of personal data derives from privacy law or the derived the refrom right to information autonomy. For this reason, it is only natural that the consent of an entitled person to process their personal data was made a top priority from among the legalizing prerequisites set forth in art. 6 para. 1 point f) GDPR. From the perspective of liberties, it is understandable as every person has, in principle, a right to manage their interests, which also includes the right to disclose one's privacy. Therefore, one's consent presents itself as universal grounds to process data, however with the significant risk for the data controller that it can always be withdrawn. The advantage of one's consent is also the fact that, when expressed, GDPR does not prescribe that the prerequisite of "necessity" be examined. So, it is hard to resist the impression that one's consent begins to be perceived as an independent and unconditional basis for processing personal data in the meaning of GDPR.

The limits of the effectiveness of consent

This interpretation, however, does not hold true as the right to privacy or the said right to information autonomy should be considered in the context of human rights, which cannot be waived but can be limited under certain conditions as long as the essence of freedoms and rights is not violated (art. 31 para. 3 of the Polish Constitution). Therefore, one's consent is only a prerequisite of admissibility to process one's data as long as other justified aims exist that allow one to invade privacy.

Such an interpretation takes account also of the GDPR regulations: in accordance with art. 5 para. 1 point b) of the Regulation, personal data are collected for legitimate purposes and "not processed in a manner that is incompatible" with those purposes (purposes limitation). This regulation is supplemented by the "data minimization" rule, *i.e.* limiting the processing with the "necessity" to the purposes (art. 5 para. 1 point c)).

Two important conclusions can be drawn from the above. First, since the purposes of processing data must be legitimate then, before the data controlled requests consent, a "legal justification of the purposes" must be evaluated. At the same time, it appears that a potential data controller's wish to exercise his fundamental rights and freedoms constitutes a justified purpose. The other conclusion is that art. 6 of GDPR gives rise to a fairly comprehensive system of prerequisites that complement one another as referred to in art. 6 para. 1 point a) (consent), art. 6 para. 1 point b) (in part where it pertains to providing data for processing necessary to conclude an agreement), and art. 6 para. 1 point f) (necessary for the purposes of the legitimate interests pursued by the controller or by a third party). All these cases discuss the legal interest of a data subject despite the fact that it occasionally overlaps with the common interest.

Let me just mention at this point the prerequisite referred to in art. 6 para. 1 point b) because it seems to be an indirect form of expressing one's consent. Pursuant to this regulation, a data subject requests ("at the request of the data subject") that his/her data be used to conclude an agreement then the data subject all the more consents to data processing. It also appears that the data subject can withdraw such a request thereby making it impossible to further process his/her data; this in essence makes the regulations similar to a large extent unless the data controlled shows the existence of other legalizing prerequisites like *e.g.* his own or a third person's interest as analysed below.

Consent and the interest of the data controller or a third party

The most interesting relation arises, however, when comparing the prerequisite of one's consent with the prerequisite under art. 6 para. 1 point f). Again, in accordance with art. 6 para. 1 point f), processing personal data is permissible if it is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child".

Let's take a closer look at the said regulation, especially at its individual components. Firstly, a legal interest must occur, rather than a factual one alone. Secondly, the interest pertains to the data controller or a "third person". Thirdly, the interest or fundamental rights and freedoms of a data subject that require protection "are not overriding" the legal interest of the data controller or a third person. And finally, the prerequisite of necessity must occur.

The key prerequisite of the regulation at hand is the concept of "legitimate interests" that has been discussed in numerous publications (Nerka, Sakowska-Baryła, 2018; Barta, Kawecki, Litwiński, 2018; Lubasz, Chomiczewski, 2018), to which the reader might wish to refer, although I treat the publications as a beginning of the discussion rather than the end of it. The initial reading of the regulation gives rise to a host of questions, including in particular the ones about the relationship between the notion and the idea of fundamental rights. Another interesting issue is why the term "interest" alone was used without the adjective "legitimate" as regards the data subject (unless it is accepted that the regulation should be read in relation to the context and assumed that it is the legal interest in this case as well) and why it was distinguished from fundamental rights and freedoms. I will not elaborate on the above matters at this point because I will adopt the safest interpretation, namely that the regulation under this analysis pertains to the conflict of fundamental rights and freedoms, which at the same time must include the protection of legal interests.

Therefore, the third prerequisite only will be discussed in this text in more detail as it follows from this prerequisite that if the interest, rights, and freedoms of a data subject are equal, then art. 6 para. 1 point f) will apply. Only overriding interests exclude the admissibility of processing data without the consent of a data subject; but we will return to this issue when analysing the institution of one's objecting to processing their personal data.

In view of the above analysis, the data subject's consent will apply only when the interests and rights and freedoms of the data subject will override the legal interest of the data controller or of a third person.

The issue of a person's "overriding" interests, rights and freedoms v. the interests of the employer

In this context, let's move on to the issues of processing employee personal data. The vast majority of processing personal data in employment relationships shall be based on the prerequisite of implementation of public tasks and performing one's legal obligations. Data processing that is based on consent or the interests of the data controller or a third person shall pertain, in my opinion, to a margin of processing cases. The need to process employees' image in various employment situations, *e.g.* I.D. badges, photographs from company events, or those published on the company's Internet sites, and also collecting personal data that is connected with competing activities, processing data in the context of trainings, or taking days off work unlawfully.

Before we analyse the most disputable case, *i.e.* one's image, we should take a good look at art. 6 para. 1 point f) in the context of labour law, in particular in the context of the employee's duty to protect the interest of the employer. From this perspective, two significant issues arise. First, how does the concept of the employer relate to the concept of data administrator and of a third person; and the other, how does one's belonging to the work establishment community relate to an entitled person's overriding interests, rights and freedoms.

Let's start with the work establishment. In its content, this concept, even in the most conservative statements, contains "community." Part of the doctrine claims that a "work establishment" includes both persons and the property. In my opinion, it is a notion that pertains to the community only, more specifically to the distinguished by law community of workers and an entrepreneur or entrepreneurs. For the purposes of this analysis, however, the above bears no significance because from every perspective a work establishment emerges as a community that has its own "interest" (art. 100 para. 2 point 4 of the Polish Labour Code) that has to be perceived as a subcategory of a larger common good — the good of society as a whole. The essence of the good of the work establishment is that all employees and the employer have a common overriding interest — the success of the organization, which allows one to maintain jobs and secure funds to be distributed between the capital and labour. In other words, the essence of the work establishment's interest is that every member of the community, *i.e.* an employee and the entrepreneur, could better enjoy their constitutional rights and freedoms thanks to the very possibilities that the community at a work establishment provides (remunerations, benefits, personal fulfilment through work, *etc.*).

Similarly to the provisions of the Polish Labour Code, GDPR refers most frequently to individual members of such a community (an employee, an employer, an entrepreneur, *etc.*). This does not change the fact, however, that in employment relations legal interests and rights and freedoms of employees and employing entities as regards the work establishment's success, are shared. Given the above, we can answer the questions posed above.

First, assuming that the data controller is the employer understood as a synonym of an entrepreneur (about which one can argue, claiming that the data controller is the employer understood as a head of an organizational unit), then his legal interest, understood as a fulfilling his dignity as a person through economic activity, as well as the legal interest of this category of third persons that are employees, understood as fulfilment of their dignity through work, is common with the interest of the work establishment and at the same time with the success thereof.

Secondly, insofar as it relates to the scope of functioning of the employee community which, as already mentioned involves also the work establishment's economic success, as a matter of principal, "overriding" of a single employee's interests and their rights and freedoms does not take place just as there is no overriding of interests, rights and freedoms of a shareholder or stockholder. Furthermore, in accordance with the theory of liberal community, *i.e.* established only so that an individual can have more real rights and freedoms, the limiting part of freedoms and rights to the benefit/in favour of a community is more advantageous/beneficial for the individual. Naturally, as in every case of restricting one's rights and freedoms, there exist limits to such interference.

The interest of the work establishment vs. recital 47 of GDPR

The above argument directly writes into recital 47 of GDPR that shows the intention of the EU legislator in the context of art. 6 para. 1 point f), specifying the conditions for the admissibility of the application of this grounds for data processing. Let's take a closer look at some fragments of the recital as it appears to be a direct description of the relationship employee — employer — other employees.

And so, from recital 47 follows that "taking into consideration the reasonable expectations of data subjects based on their relationship with the controller, the interests or the fundamental rights and freedoms of the data subject are not overriding." This should not occasion any doubt that an employee is performing work in the service at someone's direction, therefore the employee waives part of his/her freedoms, which is not only a form of accepting that some of his/her freedoms and rights are not overriding but rather those rights and freedoms are overriding that the acting with the limits of law employer represents.

The recital continues: "Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller". As I indicated above, an employee is part of the work establishment community and, in the context of the code duty mentioned above to care for the good of the work establishment, the employee acts also to the benefit of the data controller.

Obviously, the above cannot mean that upon employment all cases of data processing fall within the regulation under analysis, because there must exist a close link between data processing with its social role — one's being employed in a work establishment. Therefore, one should take into account the following fragment of recital 47: "The existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place".

The description of the employee relations complies with the requirements of recital 47 in an exemplary way. It also refers to this part of the recital which states that "the processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned". The above allows one to apply art. 6 para. 1 point f) of GDPR in those cases of abuses by employees in which there are no legal grounds to carry out an audit/check, which means that a possibility to apply other grounds legalizing personal data processing.

The special status of an employee in the context of art. 6 para. 1 point f) of GDPR is also indicated in

recital 48 concerning "a group of undertakings or institutions affiliated to a central body" which, in accordance with the recital, can have a legitimate interest in data processing for "internal administrative processes", the employees' personal data among others.

Art. 6 para. 1 point f) of GDPR as a basis legalizing personal data processing on the example of e-mail addresses and the protection of one's facial image

In the light of the foregoing, the most important element of the analysis of art. 6 para. 1 point f) of GDPR becomes the evaluation of the weight of a legitimate purpose and in the context of employee matters — the purpose of work establishment as a community that includes the entrepreneur and employees.

Let's consider this with the example of processing personal data of employees that consists in disclosing to the clients e-mail addresses in order to conduct business correspondence. While interpreting GDPR in the context of "necessity", such a practice without the consent of employees would be unacceptable. Theoretically, there is no problem in corresponding with clients from a common/joint e-mail box or in assigning the employees their e-mail addresses marked "employee 1, 2, 3" and so on, *i.e.* in anonymization of data. The content of the e-mail will reach the client anyway and the client can respond to an anonymous employee.

However, corresponding with the use of personalized e-mail addresses has at least this one advantage that the internal communication within an entity improves greatly. There is no need for "decoding" persons hiding behind anonymized data. Thus, although using e-mail addresses that identify a person by their first name and surname is not necessary, still the purpose — optimizing the flow of information and taking decisions is legitimate, which means that the intrusion in personal data is necessary and adequate. It should be added that personification of the persons who contact the environment of a work establishment has other advantages as discussed further below.

In so far as the right to disclose personal data concerning one's employment via an e-mail address is generally accepted based on art. 6 para. 1 point f), publishing photographs on Internet sites is not. Let's take a closer look at this case because it is particularly interesting. We will omit the issue of a possible need to obtain consent based on art. 81 of Law on Copyright and Related Rights (*i.e.* Journal of Laws 2018, para. 1191, as amended) and focus on GDPR alone/only.

The key question is whether an employee's personal interest, namely his/her image, is overriding the interest of the work establishment, namely the interest of the entrepreneur and other employees. For the above reasoning speaks the fact that through publishing a person's photograph together with the person's name gives rise to a possibility to identify the person in their private life long after the person ceases to be the employee.

On the other hand, it is so that carrying out certain professions or performing work in certain positions entails a natural expectation that such a person be identified. As the literature and judicial decisions indicate, an employer cannot be deprived of a possibility to disclose the data of employees who hold certain positions because it would, in an unjustified way, hinder the functioning of a work establishment and business contacts with clients, contractors, and public administration (Tlatlik, 2018, p. 21; judgment of the Polish Supreme Court of 19 November 2003, I PK 590/02, Legalis). Although the view was formulated in reference to one's first name and surname, still, in times of economic and civilization development, one should give a thought to liberalization of views about the employee image as well. Commercial operations or services are based not only on warranties arising from contractual provisions but also on trust. Obviously, in the latter aspect, nothing can replace personal contact and access to one's image is a half-measure at the very least. It may be argued that the greater the scale of distance relations the greater a role of the image of a person who acts on behalf of the business enterprise. From this perspective, the image of "frontline" employees is a significant element increasing market opportunities and influencing clients' trust toward the company.

It also seems that making the image of experts available to the public becomes a significant marketing asset in teams that offer specialist services. There is no need to carry on deep research to see the tendency on Internet sites of consultancy firms. In this sense, we can also speak of a unique/intrinsic "relativity" of the data controller's justified interest. If, in a given industry, publishing employees' images is massive, then the entity which does not publish the images of its specialist will be perceived as an organization that is "closed" and "unmodern". This "modernity" feature consists in it that in the context of voluntary and broad publishing of photographs, *e.g.* in social media, the restrictive protection of one's image in a professional context can seem incomprehensible for potential clients. Thus, an entity that "strays out" of the trend loses its competitiveness. The above means that in the name of keeping its competitiveness the employer can process the images of its employees based on art. 6 para. 1 point f) because the rank of the legal interest of the entire work establishment grows together with the standards of actions of its environment in which the work establishment operates.

In reference to the above, I wish to point out that arguments for the admissibility of processing employee images in the open Internet space without data subject's consent (omitting consent under copyright law) pertain

to very specific groups of employees, primarily to leaders of organizations. The matter must be treated individually, however, and it should not be excluded that publishing the images of line employees constitutes market value that lends credence to the reliability of the company's operations.

The right to use the image of an employee is, in my view, even broader for the purposes of internal communication, both to identify a person and for its use in the intranet. By "internality" I understand also the communication in capital groups. Consequently, I view the position of the Personal Data Protection Office (PDPO) as too conservative: in the context of admissibility of using photographs on ID badges, requires consent from the employee. I believe that in the name of improving internal communication and at times to ensure client's security, it is justified to process personal images under art. 6 para. 1 point f). The above pertains in particular to large entities with great employee turnover, or entities that are strongly engaged in international cooperation, *etc.* Only a closer analysis of the factual state can lead to the answer as to which one is more important: the aforementioned values for organizing teamwork or the individual right of an employee. Furthermore, the more an organization is closed for third persons, the fewer arguments speak for it that a personal interest of an employee overrides the rights of an entrepreneur or other employees.

A completely different thing is whether, in the name of minimizing personal data, the photographs of the employees should be always saved in the employer's electronic collections or resources. The duty to wear an ID badge can be imposed through a provision in the employee handbook, thereby transferring the ownership of the badge onto the employee without processing photographs in the employer's resources. In such a case, GDPR would not apply at all. One should keep in mind, however, that the principle of proportionality applies to every legal act, thus to the employee manual as well. In other words, imposing the duty to wear ID badges with a photograph unjustified by proportionate needs will be violating law even when the employer would not process images as a data controller and thus GDPR would not apply.

Returning to GDPR, however, it seems that, in the dominating majority of cases, processing personal data in the context of ID badges will be based on art. 6 para. 1 point f) rather than on the necessity to obtain consent. The above is consistent with the views on identifying persons through their image in intranets, in which case such a possibility is quite commonly admissible without the employee's giving their consent. However, doubts have been voiced in reference to large entities, which employ hundreds of employees, especially those that are part of an international corporation, where the number of recipients is very vast (Tlatlik, 2018, p. 21). It appears, however, that closing the circle of persons having access to the image excludes the argument of dissemination. A similar conclusion can be drawn about employee ID badges worn within a work establishment.

And yet, problems with processing images exceed a simple placing of one's photograph on a badge. A "work establishment's life" also consists of internal ceremonies and official events. A number of arguments exist for saying that processing data from local events in intranets and from official events (beginning of an investment project, commencement of a production, anniversary of a product, *etc.*) and also in open networks is based on art. 6 para. 1 point f) of GDPR. It is especially the case where photographs do not bear a description that allows one to identify the persons in them.

As I mentioned above, a work establishment is a community whose natural functioning cannot be paralyzed by individuals' resistance unless they show a specific and material right or freedoms that override building social relations. What is more, this remark also refers to non-employees who participate in the life of a work establishment, like the employees' relatives.

Protecting human dignity

As already mentioned, an individual's belonging to the community of their work establishment is connected to it that less often than in private relations a person's interests, rights, and freedoms will override the interests of the work establishment and, more frequently than not, the opposite will be true. This means that, in the name of the employer's using art. 6 para. 1 point f) of GDPR, a duty can be imposed on an employee, for instance, to participate in a photo session. Furthermore, the employer may express expectation that an employee express consent that is required by copyright law where it is necessary, which makes the voluntariness illusory. Should it be assumed that the weight of publishing one's image was so significant that it justifies data processing under GDPR without the employee's consent, the refusal to participate or giving consent referred to in art. 81 of copyright law would have to, in extreme cases, be found as a justified reason for termination one's employment agreement, and such interpretation may stir objection as being anti-freedom. It appears, however, that the Labour Code includes regulations that mitigate the above tension and allow employee candidates and employees to make rational choices. GDPR does not release the employer from the duty to care for employee's dignity and their other personal interests under art. 11^1 of the Labour Code. In my opinion, at least three significant specific duties of the employer's can be derived from the above provision of law.

The first is that candidates for employment should be informed about the fact that at the post they apply for a cooperation with the employer is expected as regards processing some personal data and that their

refusal can have a negative effect on their further employment.

The second duty is that persons who are already employed should be informed about whether their participating in work establishment events may entail processing their data pertaining to their image, irrespective whether copyright law requires their consent or not and irrespective of it whether collected data will allow one to identify such persons or not.

The third duty is that employer exercising his entitlement arising from art. 6 para. 1 point f) of GDPR should be excluded toward those persons who should show that their personal situation is particularly sensitive; in other words, that the interests of the work establishment does not constitute a value that is greater than the interest, rights, and freedoms of such a person.

Apart from the interpretation of art. 11^1 of the Polish Labour Code, the above reasoning has more value. Let's recall that in the examination of the reasons for the application of art. 6 para. 1 point f) in the context of recital 47, we indicated that GDPR expects the person linked to the data subject linked to the data controller should have "reasonable expectations" concerning the fact that his/her interests, rights and freedoms do not override the interests of the data controller of third persons. Performing the actions described above and derived from art. 11^1 of the Labour Code increases the range of cases in which the "reasonable expectation" will take place.

Final remarks

In the above text, I have focused on the exceptionally sensitive matter concerning one's image in the context of the work establishment's interests. art. 6 para. 1 point f) of GDPR provides arguments for processing certain data in capital groups because the interests of a work establishment are closely linked to such groups' success. In any case, the EU law has long noticed the existence of an overriding community of interests by introducing the Directive on European Works Councils.

The regulation under this commentary allows one to process employees' personal data in the context of non-mandatory training; it justifies transferring contact personal data to third persons, to mark premises by providing personal data, to order handing away business cards, to collect data about a person abusing rights or violating law toward the employer, to conduct controls of an employee, *etc.*

The above text does not prejudge in detail about the admissibility of every one of the above cases. In particular, exceptional caution should be taken if one's image is to be processed in the public domain. This is so because this analysis has two aims: firstly, to show that employee's consent as a prerequisite for processing their personal data will have a marginal application and, secondly that, in the context of the interests of a work establishment, the application of art. 6 para. 1 point f) of GDPR to processing personal data in close connection with the operations of the work establishment will be generally stable because, in the competition between the interests of the work establishment (behind which there is the interests of the entrepreneur and other employees) and the interests, rights and freedoms of an employee, the former one will frequently have an overriding significance, which will justify processing an employee's personal data despite his/her objection.

Bibliography

Barta, P. Kawecki, M. Litwiński, P. (2018). In: P. Litwiński (ed.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*. Warszawa: Legalis.

Lubasz, D. Chomiczewski, W. (2018). In: E. Bielak-Jomaa, D. Lubasz (ed.). *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*. LEX.

Nerka, A. Sakowska-Baryła, M. (2018). In: M. Sakowska-Baryła (ed.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*. Warszawa: Legalis.

Tlatlik, J. (2018). Pracownicze prawo do wizerunku jako przedmiot ochrony prawnej. *Monitor Prawa Pracy*, (10).