OFFICE FOR THE PROTECTION OF PERSONAL DATA OF THE SLOVAK REPUBLIC

Hraničná 12, 820 07 Bratislava 27

No.: 00204/2018-Op-3

Methodological guideline no. 3/2018 Obligations of the e-shop operator from the point of view of personal data protection

Updated version from 02/18/2020

According to § 81 par. 2 letters d) Act no. 18/2018 Coll. The Personal Data Protection Office of the Slovak Republic (hereinafter referred to as the "Office") issues this methodological guideline.

INTRODUCTION

The purchase of goods and services is currently carried out to a large extent via the Internet. An online store (hereinafter referred to as "e-shop") can be defined as the sale of goods or services using information and communication technologies and web applications in the Internet environment, where the e-shop operator is on one side of the relationship and the e-shop customer is on the other (hereinafter referred to as "customer"). The most common among them is the conclusion of a purchase contract realized via the Internet (a contract concluded at a distance). The acquisition of information, including the customer's personal data, is part of such a contract.

Due to the dynamism of the development of information technologies, it is impossible to take into account in this methodological guideline all eventualities that could arise when the e-shop operator applies the Regulation, therefore the office lists below only the most common cases. Considering the specific conditions of the processing of personal data, it is possible that the e-shop operator will be able to use e.g. also a different legal basis or settings other than those listed below. This methodological guideline is only a recommendation of the office, i.e. from. that it does not exclude other settings for the processing of personal data subject to the fulfillment of all the conditions and obligations established by the Regulation.

At the outset, it is also necessary to emphasize that other special regulations also apply to the issue of e-shops, e.g. Act No. 351/2011 Coll. and Act No. 22/2004 Coll., which must be taken into account when operating e-shops. These regulations do not belong to the substantive competence of the office.

1. PROCESSING ACTIVITIES OF THE E-SHOP OPERATOR AND LEGAL BASIS FOR THE PROCESSING OF

CUSTOMERS' PERSONAL DATA Recording the personal data of a customer of a particular e-shop is, from the point of view of the personal data protection rules, the processing of the customer's personal data. The purpose of such processing is most often the conclusion of a purchase contract and the subsequent payment, delivery of goods or services, and possibly the provision of other related services (complaints and other obligations for the operator of the e-shop resulting mainly from legal regulations governing consumer protection).

It is necessary to distinguish between the individual purposes of processing customers' personal data by the e-shop operator. With regard to these purposes, we can identify several of the most common processing activities, which may be closely related, but have a different legal basis.

The processing of personal data of customers by the e-shop operator takes place mainly for the purposes of:

order of goods/services (e-shop) → purchase contract according to Art. 6 par. 1 letter b) Regulations (subsequent payment, delivery of goods or services, processing of complaints, etc. are also related to this); the processing of the customer's personal data takes place without the customer's consent, since the legal basis for the processing of his personal data for the purpose of fulfilling the contract is a specific contract concluded at a distance between the customer and the e-shop,

marketing communication with the customer → legitimate interest according to Art. 6 par. 1 letter f) Regulations (e.g. newsletter sending, other forms of direct marketing, etc.); the processing of the customer's personal data takes place without the customer's consent, since the legal basis for the processing of his personal data (to the extent necessary) is the legitimate interest of the e-shop operator, for example informing the customer about new goods and services of the given e-shop in order to promote their sales,

marketing communication with the person concerned without a previous relationship →

prior consent of the person concerned according to Art. 6 par. 1 letter a) Regulations,

loyalty program → consent6 of the customer according to Art. 6 par. 1 letter a) Regulations,

consumer competition → consent6 of the customer according to Art. 6 par. 1 letter a) Regulations.

2. OBLIGATIONS OF THE E-SHOP OPERATOR

Compliance with the principles of processing personal data of customers according to Art. 5 Regulations

in order for the operator to be able to legally process the personal data of customers for the aforementioned purposes, it must have an adequate legal basis (see point 1) (principle of legality),

customers have the right to be informed about the conditions of processing, the manner in which their requests for the exercise of the rights of the affected persons are handled, etc. (principle of transparency),

the operator should process the obtained personal data only for a specifically defined, explicitly stated and legitimate purpose, and they may not be processed in a way that is not compatible with such a purpose (principle of purpose limitation),

the operator shall process only such personal data as are necessary to achieve the specific purpose of processing (principle of data minimization), for example:

to conclude a purchase contract - e.g. title, name, surname, address of residence, address of delivery of goods, if it is different from the address of residence, e-mail address, telephone number,

for direct marketing – title, first name, last name and e-mail address,

loyalty program – title, first name, last name, residential address or e-mail address and possibly other data (for example, depending on how the benefits from the loyalty program are provided, or depending on other conditions of participation in the loyalty program set by the operator),

consumer competition – the list of processed personal data depends on the conditions of the competition specified in the competition statute, about which the affected persons should be informed before granting consent to the processing of their personal data for the purpose of the competition,

the operator processes correct and updated personal data (correctness principle),

the operator stores personal data only for the necessary time to achieve the purpose of processing; longer only if it is necessary for another purpose (for example, for the purpose of archiving) compatible with the original purpose (minimization of storage principle),

the operator guarantees adequate security of processed personal data (principle of integrity and confidentiality),

the e-shop operator must be able to demonstrate compliance with the previous processing principles (responsibility principle).

Information obligation according to Art. 13 and Art. 14 Regulations

applies to all processing activities mentioned in point 1; the obligation to provide information goes from the operator of the e-shop to the affected person (customer of the e-shop),

providing information to the affected person is the operator's obligation, i.e. the e-shop operator is obliged to fulfill it proactively (not based on the request of the affected person),

the operator provides the person concerned with the information provided for in Art. 13 par. 1 to 3 of the Regulation, if he obtained personal data directly from the person concerned; according to Art. 14 par. 1 and 2 Regulations, if he did not obtain personal data directly from the person concerned [example: person X orders in the ABC e-shop, a product purchased as a gift for person Z. The ABC e-shop processes the personal data of person X on a contractual legal basis and fulfills its information obligation according to Art. 13 Regulations. The ABC e-shop also processes delivery personal data about person Z, who does not know that a gift will be sent to him, while there is no direct contractual relationship between ABC e-shop and person Z. The legal basis for the processing of personal data of person Z will thus be the legitimate interest of e-shop ABC for the purpose of fulfilling the contract between e-shop ABC and person X. E-shop ABC will also fulfill its information obligation towards person Z according to Art. 14 Regulations. Since in this situation the exception according to Art. 14 par. 5 letters b) Regulations ("... or if it is likely that the obligation referred to in paragraph 1 of this article will make it impossible or seriously difficult to achieve the goals of such processing"), e-shop ABC fulfills the information obligation according to Art. 14 He will fulfill the regulations towards person Z only at the moment of delivery of the gift purchased by person X],

to apply exceptions from the information obligation only to the extent defined in Art. 13 par. 4 and Art. 14 par. 5 Regulations,

in relation to new customers from 25/05/2018 - to fulfill the stated information obligation at the latest when obtaining personal data,

in relation to already existing customers before 25/05/2018 (e.g. with regard to ongoing marketing, loyalty program) – obligation to add information to the extent that the customer does not have information according to Art. 13 and Art. 14 Regulations,

provide information in a concise, transparent, comprehensible and easily accessible form, formulated clearly and simply,

can be informed in different ways (also combined) - e.g. on the website of the e-shop, by sending information to an e-mail, in paper form in the premises of the "stone store", etc.,

the operator informs its customers of their rights as a data subject (Articles 15 to 22 of the Regulation), in particular the right to object to processing for direct marketing purposes and the right to withdraw consent to processing,

if the processing is based on a legitimate interest, the operator informs the customer about which legitimate interests it pursues; the operator is also obliged to carry out a proportionality test whenever it processes personal data on this legal basis.

Keeping records of processing activities

 every e-shop operator is obliged to keep records of processing activities according to Art. 30 Regulations always in relation to

processing activities:

order of goods/services

loyalty program

direct marketing

! CONSUMER COMPETITION

if it regularly organizes competitions

 if he occasionally organizes a competition - e.g. 1x/year and so on. (the exception according to Article 30, paragraph 5 of the

Regulation applies and this processing activity does not have to be mentioned in the record)

 the operator keeps the records with himself and does not send them to the office, if applicable

submits them to the office for inspection.

Responsible person

e-shop operators who meet the condition according to Art. 37 par. 1 letter b) Regulations - e.g. if behavioral advertising is

carried out,

if the condition according to Art. 37 par. 1 letter b) The regulations are not fulfilled, the operator of the e-shop is not obliged to

designate a responsible person; if he nevertheless voluntarily designates it, he is obliged to proceed in the same way as if the

obligation to designate a responsible person applied to him.

Intermediary

the operator can entrust the processing or part of the processing to an intermediary, for example for the purpose of evaluating

a competition organized by the operator, sending satisfaction questionnaires with purchased goods, etc.,

the intermediary processes personal data according to the instructions of the operator, to the extent and according to the

intermediary contract or other legal act12, which binds the intermediary towards the operator. The intermediary contract and

other legal act must meet the requirements according to Art. 28 par. 3 Regulations,

for the purpose of concluding an intermediary contract and authorizing the intermediary to process personal data, the consent

of the person concerned is not required. In terms of legality, the intermediary has the operator's legal basis for processing

personal data (e.g. legitimate interest).

Security of personal data processing

the operator of the e-shop is responsible for the security and protection of personal data for the entire time of their processing and is obliged to take appropriate security measures for their protection,

according to Art. 25 of the Regulation, the e-shop operator is obliged to ensure protection already at the stage when the processing has not yet started, while taking into account the latest knowledge and the costs of implementing measures as well as the nature, scope, context and purposes of the processing. It sets the measures according to the needs in relation to its own environment and takes into account the safety standards that are common for this or that processing activity - e.g. secures the computer on which the customer's personal data is processed with an anti-virus program,

according to Art. 32 of the Regulations, the e-shop operator is obliged to take appropriate technical and organizational measures in view of the above:

technical measures – antivirus, firewall, password-protected computer, alarm, object security, security of automated and non-automated means, etc.

organizational measures - instructions of the e-shop operator addressed to employees (if any), designation of the responsible person (if he has an obligation

to determine it), instructing employees to maintain confidentiality, mode of entry to premises where personal data is processed, key policy, rules for processing personal data, including rules for their storage, etc.

 the listed measures are only examples, it is not possible to generalize the necessary measures for all e-shops

the operator is obliged to carry out an assessment of the impact on data protection according to Art. 35 of the Regulations, if it fulfills any of the conditions established in this article,

! in the event of a breach of personal data protection that will lead to a risk for the rights and freedoms of natural persons (e.g. making a database with personal data of customers available to unauthorized persons or damage and unavailability of the e-shop operator's backups), such breach within 72 hours after the he learned to report this fact to the office; in some cases also to the person concerned, without undue delay. 15

 The operator of the e-shop may comply with Regulation and Act no. 18/2018 Coll. can also be demonstrated by observing a code of conduct or a certificate, but it is not the operator's obligation to adhere to such a code of conduct (if it exists), or apply

for a certificate.

Regarding other obligations, please note that the operator of the e-shop is also obliged to fulfill the obligations pursuant to Act no. 351/2011 Coll. on electronic communications as amended (hereinafter referred to as "Act No. 351/2011 Coll."). To interpret the provisions of Act no. 351/2011 Coll. the office is not materially competent, we recommend contacting the legal representative.

3. STATUS OF THE E-SHOP CUSTOMER AS AN AFFECTED PERSON

From the point of view of the Regulation, the e-shop customer is a data subject, i.e. a natural person to whom the personal data processed by the e-shop operator relate. According to the Regulation, the person concerned has rights that he can exercise against the operator of the e-shop at any time.

What rights does the affected person have?

Right of access to data (Art. 15)

Right to correction (Art. 16) Right to erasure (Art. 17)

Right to restriction of processing (Art. 18)

Right to portability (Art. 20)

Right to object (Art. 21)

if the processing is carried out based on the legitimate interest of the e-shop operator (e.g. for direct marketing purposes), the customer has the right to object to such processing of his personal data at any time,

the right to object for the purposes of direct marketing must be explicitly notified to the person concerned at the latest in the first communication with him and this right must be presented clearly and separately from any other information,

after applying the customer's objection, the e-shop operator is obliged to immediately end the processing of personal data for the purposes of direct marketing and to no longer process these personal data for the purposes of direct marketing.

 Right to withdraw consent

if the processing takes place on the basis of the customer's consent (e.g. loyalty program, consumer competition), the customer can withdraw his consent to the processing at any time and the e-shop operator is obliged to stop the processing of personal data that was processed on the basis of consent, if there is no other legal basis ,

if the processing is carried out on the basis of the customer's consent, the customer must have the right to revoke the consent

at any time according to Art. 13 par. 2 letters c) Regulations by the e-shop operator informed in advance.

How should the operator proceed when handling the requests of the persons concerned?

it is recommended to prepare a short, clear and concise internal procedure for how the e-shop operator will handle the requests of affected persons (e.g. in the form of an internal directive, an instruction), which can be published on the website of the e-shop operator

(the operator can create a sample form),

all information and notices of the operator towards the affected person must be in a concise, transparent, understandable and easily accessible form, formulated clearly and simply, the category of affected persons to whom the notices and information are addressed must be taken into account,

as a rule, information and notices should be provided in the same way in which the affected person exercises his right, unless he requests another way,

the operator of the e-shop is obliged to process the request of the affected person within 1 month of its delivery (if necessary, the operator can extend the processing of the request by another 2 months, while he is obliged to notify the affected person of the extension of the deadline).

4. TECHNICAL ASPECTS OF E-SHOP OPERATION IN THE CONTEXT OF PERSONAL DATA PROTECTION

4.1 E-shop template

When choosing a technical solution for an e-shop template (an interface used to browse specific goods offered in the e-shop or to add individual items to the so-called "basket"), the operator of an e-shop can basically proceed in two ways. Either he creates the e-shop template himself or he can (e.g. through a license agreement) acquire an e-shop template from another entity. In most cases

from the point of view of personal data protection, personal data is not processed by the provider of such a template.

4.2 Web hosting of the e-shop

If the operator does not have its own web space for the technical operation of the e-shop, it most often enters into a contractual relationship with the entity that provides it with such a space. The position of the web space provider will then depend on how the conditions are set.

If this entity provides a web space for the e-shop operator without processing the personal data of the e-shop customers,

which the e-shop operator processes, there will be no need to adjust their mutual relationship from the point of view of personal data protection.

If personal data of e-shop customers will also be processed through a web space provider, this provider will act as an intermediary according to Art. 4 par. 8 Regulations, if the web hosting provider will process personal data on behalf of the operator. The mutual relationship between the e-shop operator and the web hosting provider will be governed by a contract or other legal act according to Art. 28 par. 3 Regulations.

The provider of the web space can also have the status of a joint operator, if it occurs, e.g. to automatically back up data from the e-shop. In such a case, when adjusting the relationship between joint operators, i.e. the relationship between the e-shop operator and the web space provider, the procedure is in accordance with Art. 26 Regulations.

4.3 Technical support provided to the e-shop operator by a third party

If a third party provides technical support for the e-shop, when during the elimination of technical problems can this entity, or its employees can see the personal data of e-shop customers and there is no further processing of personal data by the entity performing technical support (i.e. it only "sees" personal data, but does not process it further) it is sufficient for it to be in the contract between the operator and the technical support provider established obligation to maintain confidentiality and take adequate security measures (organizational and technical). The above also applies in relation to the implementation of technical support via remote access.

5. OTHER POSSIBILITIES OF PERSONAL DATA PROCESSING DURING THE OPERATION OF THE E-SHOP

5.1 Recipients in the case of an e-shop

In the case of e-shops, the recipients are e.g. courier companies. They can deliver goods ordered in the e-shop to the customer either in their own name and under their own responsibility, when as independent operators they must have an adequate legal basis and comply with other obligations according to the Regulation or on behalf of the operator of the e-shop, when they act as an intermediary.

In the process of processing personal data of customers by these recipients for the purpose of delivering ordered goods, it is necessary to distinguish between those who provide their services according to Act no. 324/2011 Coll. on postal services and on the amendment of certain laws as amended (hereinafter referred to as "Act No. 324/2011 Coll.") and by those who do not comply with this Act.

In the case of couriers or delivery companies (hereinafter referred to as "deliverers") who do not comply with Act No. 324/2011 Coll., it is necessary to distinguish situations,

when a delivery/transportation service is ordered directly from the person concerned, when the legal basis for processing the personal data of the person ordering the service is a contract between the person concerned and the delivery person (see example no. 1),

when a delivery/transportation service is performed based on the selection of such a service directly in the e-shop environment for the purpose of delivering the purchased goods, when the legal basis of the delivery person will be the consent of the buyer (see example no. 2) and

when the delivery/transportation service takes place on the basis of an e-shop instruction, when the legal basis is a contract between the customer and the e-shop (see example no. 3).

[example no. 1: the KKK e-shop sells clothes. The legal basis for processing the customer's invoicing data will be the purchase contract directly between the KKK e-shop and the customer. The KKK e-shop offers a choice of two types of goods delivery, namely personal collection at the branch and delivery by delivery man Q or delivery man H. The customer has a bad experience with delivery man Q, and therefore decides to use the services of delivery man H. Since the KKK e-shop and the delivery man H have set the terms and conditions so that the customer is directly linked to the website of the delivery company H, where the customer chooses the day, time of delivery as well as the complaint conditions, the legal basis of the delivery company H will be the contract and not consent. In this case, the deliverer as well as the KKK e-shop are separate operators.]

[example no. 2: LUL e-shop sells mobile phones. The legal basis for processing the customer's invoicing data will be the purchase contract directly between the LUL e-shop and the customer. The LUL e-shop offers a choice of three types of goods delivery, namely personal pick-up at a branch, delivery of goods by post or courier. The customer decides that the goods will be delivered to him by the courier as quickly as possible, and therefore ticks the box by which he gives consent to the courier to process personal data for the purpose of the delivery service. In this case, the deliverer as well as the LUL e-shop are separate operators. The e-shop and the delivery person will adjust the contractual arrangements on the conditions for complaints about damage to the goods during the transport of the goods separately.]

[example no. 3: WOW e-shop sells computer accessories. The legal basis for processing the customer's invoicing data will be the purchase contract directly between the WOW e-shop and the customer. At the same time, the WOW e-shop also delivers

goods using its own vehicles, but sometimes also uses external deliverers. However, when ordering goods, it does not give customers a choice whether the goods should be delivered to them by their own vehicles or by an external delivery person. The WOW e-shop thus determined the purpose, terms of the contract, contractual arrangements and means of processing the customer's personal data for the delivery of goods. The delivery person, who occasionally arranges the delivery of the customer's goods, processes the customer's personal data on behalf of the operator, which is the WOW e-shop, and on the same legal basis (a contract with the person concerned). The delivery person acts as an intermediary of the WOW e-shop.] courier providing services according to Act no. 324/2011 Coll. – legal basis = legitimate interest arising from the special Act no. 324/2011 Coll. according to Art. 6 par. 1 letter f)

Regulations (valid only in relation to personal data established in § 11, paragraph 1 of Act No. 324/2011 Coll.)

courier not providing services according to Act no. 324/2011 Coll. – legal basis = consent according to Art. 6 par. 1 letter a) Regulations/contract according to Art. 6 par. 1 letter b) Regulations / legitimate interest according to Art. 6 par. 1 letter f) Regulations; (as mentioned in the example above in the information obligation)

If the courier company uses, in addition to its employees, couriers who are self-employed/self-employed for the delivery of parcels, these individual couriers will have the status of intermediaries vis-à-vis the courier company on whose behalf they deliver, and it is necessary to adjust their relationship with the courier company in accordance with Art. . 28 Regulations.

5.2 Cross-border processing/transfer of personal data of e-shop customers

If the e-shop operator transfers personal data of customers to third countries, it is necessary to indicate these countries in the record of processing activities7 [Art. 30 par. 1 letter

e) Regulations] The member states of the European Union and the states that are parties to the Agreement on the European Economic Area are not third countries, so there is no need to mention them in this section, they are mentioned only in the "recipients" section [Art. 30 par. 1 letter d) Regulations].

The operator of the e-shop is obliged to inform the affected persons about these facts according to Art. 13 par. 1 and Art. 14 par. 1 Regulations.

5.3 Special ways of processing personal data by the e-shop operator

With the development of various technologies, new ways of processing personal data of customers, especially of larger e-shops, have developed over time. Below we present a few practical examples together with the legal basis for processing

personal data.

wishlist

the registered customer has the opportunity to include the selected goods in the so-called wishlist

sending an e-mail with a notification that the goods included in the wishlist are sold at a discounted price or are available again

 if it is within marketing activity – legal basis = legitimate interest according to Art. 6 par. 1 letter f) Regulations

abandoned basket

- the registered customer has not completed his purchase, he has not completed the payment and he is sent an e-mail with a warning and the contents of the basket

 no purchase contract has yet been concluded, legal basis = pre-contractual relations according to Art. 6 par. 1 letter b) Regulations

customer holiday tracking

- legal basis = legitimate interest according to Art. 6 par. 1 letter f) Regulations

reactivation

- the registered customer is no longer active in the e-shop; the operator of the e-shop will send him a code with a discount for his next purchase with the intention of motivating him to make another purchase

if it follows/is agreed in the contract – legal basis = contract according to Art. 6 par. 1 letter b) Regulations

if it is within marketing activity – legal basis = legitimate interest according to Art. 6 par. 1 letter f) Regulations

segmentation

based on what the customer buys in the e-shop, the e-shop operator sends newsletters to the customer with information about similar goods that the customer buys in the e-shop

legal basis = legitimate interest according to Art. 6 par. 1 letter f) Regulations

upselling

based on the contents of the customer's basket/or on the basis of the goods he has already purchased in the given e-shop before, when completing his order (in the payment process), the merchant will display the goods recommended by the merchant for his next purchase

legal basis = legitimate interest according to Art. 6 par. 1 letter f) Regulations

cookies - are not personal data under all circumstances; personal data is when it is part of a chain of other data related to a specific natural person, on the basis of which this natural person can be identified

cookies as personal data – depending on the circumstances of a specific case, it may be a legal basis consent according to Art. 6 par. 1 letter a) Regulations contract according to Art. 6 par. 1 letter b) Regulations

 legitimate interest according to Art. 6 par. 1 letter f) Regulations (marketing purposes)

at the same time, the obligation to fulfill the conditions according to § 55 of the Act also applies

no. 351/2011 Coll.

if cookies are not personal data - the obligation to fulfill the conditions according to Act no. 351/2011 Coll.

CONCLUSION

Processing personal data in the e-shop is relatively simple and clear after understanding the basic principles and rules of processing personal data. The operator of the e-shop must not neglect four basic areas when dealing with the processing of personal data; the first area is the legal basis of the processing, followed by the fulfillment of the obligation to keep records, the fulfillment of the information obligation towards the affected persons - customers, and last but not least, ensuring the security of the processed personal data.

In Bratislava, on October 4, 2018

Soňa Pőtheová v. r.

chairperson of the office

2