**30 steps to comply with the new data protection legislation**

**Introduction**

Provide specific guidance on how to comply with the Regulation / law.
The GDPR is a big project and requirements are not only a set of explicit met requirements, but in line with the new approach to accountability
the operator is obliged to prove compliance with the whole at any time
Regulation / Act no. 18/2018 Coll.: Starting with the basic principles of processing to for security in the processing of personal data.

We recommend planning the implementation in several steps. The first step is
getting acquainted with the content and requirements that Regulation and Act no. 18/2018 Coll. puts it on operators and intermediaries. This notification will alert you to
differences in ongoing processes compared to the requirements imposed on entities
in accordance with the current legal regulation. Act no. 122/2013 Coll.
operators who are still in accordance with Act no. 122/2013 Coll. on protection
personal data, the new legislation will not be a revolution, but rather
evolution in the field of personal data protection and operators can continuously
continue to process personal data, taking into account some new ones
institutes and responsibilities.

**1. Familiarization with basic concepts**

- What is personal information?

who is the person concerned, when a natural person is identified in my environment, or
identifiable to be crossed by personal data protection legislation

who is the controller, is who determined the purpose and means of processing and who
processes the personal data of data subjects in its own name? The operator is
responsible for compliance with the processing of personal data. The
influence and bear strict responsibility for the processing of personal data. Processing
personal data may also be imposed on the controller directly by law.

- who is the intermediary, is the one who processes personal data on behalf of
operator, according to his instructions and to the extent and according to the intermediary
contract or other legal act which binds the intermediary towards
operator? The brokerage contract and other legal act must comply
requisites according to Art. 28 par. 3 Regulations / § 34 par. 3 of Act no. 18/2018 Coll.

**2. Preparatory phase of implementation** - setting up a project team, the scope of which
is to determine the responsibilities and competencies of individual team members.
An initial analysis will be carried out, including a mapping of the current processing of personal data
data. Areas of personal data processing will be defined - here is the agenda,



the area or process in which personal data are processed, for example
population register, client database, personnel and payroll of employees.

**3. Where are we and where do we want to be?** This means analyzing the current situation, p
in order to compare where the operator is compliant and where, on the contrary, it is in conflict with
required level of personal data protection.

**4. Description of the organizational structure of the operator** - reference to the existing one
organizational rules, internal regulations and directives, also related to the issue
personal data protection or security management. He management rules and
archiving, fire, evacuation plan, complaint procedure. This documentation may
be the basis for a new privacy policy.

**5. By what means is the processing of personal data processed?**
Means of processing are defined as the procedures chosen for a particular treatment,
tools that will be used in the processing of personal data. Operator
evaluate their safety and condition. The legislation applies to the processing of personal data
data performed by:
- *completely*, at the processing are used only in technology (eg. The application) or
- *partially*, in the processing combined technology and work
human factor (e.g. filling in an Excel spreadsheet) and
- and for processing by *means other than automated means*, ie manually,
*e.g. collection of completed paper applications, management of employment contracts*
in paper form; *in the case of personal data which form part of*
*information system or intended to form part of an information system*
system.

**6. What type of personal data do I process?** We differentiate between three types of personal data:
- common (general) personal data e.g. name, surname, address, birth number.
The conditions under which processing is lawful are defined in Art. 6 par. 1
Regulations / § 11 par. 1 of Act no. 18/2018 Coll.
- *specific categories of personal data*, *e.g.* health data. biometric data.
The conditions under which the processing of such sensitive data is permitted are
defined in Art. 9 par. 2 Regulations / § 16 par. 2 of Act no. 18/2018 Coll.
- personal data relating to the admission of guilt for *criminal offences and misdemeanors* .

**7. Identify the categories of persons concerned** - e.g. clients, patients, competitors,
citizen, suppliers, vulnerable group of affected persons - minors, pensioners,
employees.

**8. Identify the purpose for which I will process this personal data.** The purpose
we mean a clearly defined or established intent for processing
personal data which is linked to a specific activity. Simply put - a specific goal
which I want to achieve by processing.



**9. To be able to describe the whole life cycle of personal data** - from the moment of their acquisition
until their disposal.

**10. Analysis of the basic principles of processing** - many subjects omit that
the security of processing itself begins with the basic principles. Principles
processing personnel to throughout the legislation and it is necessary to build on them
in the interpretation and application of individual provisions.

**11. On what legal basis do I process personal data and what processing data**
**I continue to perform operations with them.** The operator must for each processing purpose
have an adequate legal basis in accordance with Art. 6 par. 1 Regulations / § 11
par. 1 of Act no. 18/2018 Coll., Which defines the conditions under which it is
legal processing. The legal bases need to be revised and updated
many legal bases regulated in Act no. 122/2013 Coll., e.g. direct marketing
based on legitimate interest, the provision of personal data to unlimited personal data, one-off
entrance, monitoring of areas accessible to the public

**12. How was the consent to the processing of personal data obtained?** For personal data,
which are processed with the consent of the persons concerned to assess whether the consent
granted under Act no. 122/2013 Coll. meets the conditions of a validly granted consent
according to Regulation / Act no. 18/2018 Coll., So that the operator can continuously
continue with the consent of the data subject to the processing of personal data.

**13. Identification of beneficiaries, including intermediaries** - an audit will be carried out
brokerage contracts/mandate agreements/joint or
preparation of new contractual documentation in accordance with the requirements of the new legal
adjustments. A revision of the legal bases will be carried out with regard to the provision or
making personal data available to other operators.

**14. Who has access to personal data and under what authority?** Who is
how is the environment of the operator or intermediary comes to
contact with personal? Has the operator's instructions on how to handle it
with personal data?

It is ensured that these individuals have access only to the data they need
for the performance of their tasks? If you do not create barriers, be the so-called Chinese walls.

An effective mechanism for monitoring compliance with directives and internal guidelines will also be put in place
to ensure compliance with the principles of the processing of personal data, e.g. annual / semi - annual
audit, continuous control of employees at the workplace, what documents employees
take out of the workplace, etc. The human factor is generally the most common cause
security incidents.

**15. The operator and the intermediary shall** take steps to ensure that
the obligation for any person acting under the **authority of the** operator; or



intermediary (this may also mean an **authorized person** acting **for**
operator or intermediary) and has access to their personal data
processed only on the basis of the **operator 's instructions** *(extra-formal obligation*
*in the context of Art. 32 par. 4 Regulations and Art. 29 Regulations / § 39 par. 4 of Act no. 18/2018*
*Z. z.) and § 36 of Act no. 19/2018 Coll.)* Or in accordance with a special regulation or
international treaty by which the Slovak Republic is bound and at the same time, in the sense of
§ 39 of Act no. 18/2018 Coll. it remains the case that the operator and the intermediary are
shall be bound by the obligation of **professional secrecy** of the persons of natural persons who come to
contact with personal data with the operator or intermediary.

**16. The operator will provide training to raising of employees** - in the area
protection of personal data, with the aim of continuously raising awareness of the
issues in the internal area of 0.5-1 years and always at the beginning of employment.

**17. Information obligation** - to the extent pursuant to Art. 13 or Art. 14 Regulations / § 19
set § 20 of Act no. 18/2018 Coll. affects every **operator** - regardless of
whether the personal data were obtained from the data subject or from another source and without
regardless of the legal basis on which the controller processes personal data.
data. The most common way of communicating with the person concerned will be evaluated - in person, e.
by e-mail, through the website. Employees who are already in accordance with the law
no. 122/2013 Coll. have fulfilled the information obligation towards the persons concerned are obliged
to continue in the provision of information in accordance with the new information,
for example, by addressing the public through a website, or
by sending a notification e-mail. In addition to the information obligation, e.g. contact
details of the operator, contact details of the operator's representative, if authorized,
contact details of the responsible person, more specific information on rights is required
persons concerned and others.

**18. The method of handling the agenda of the rights of the persons concerned** will be **ensured - it** will be evaluated
readiness to exercise new rights on the part of the persons concerned. Operator
must provide a form for exercising rights, which will facilitate the processing of applications of the persons concerned,
ideally through dedicated sample forms, or provide
the data subject the possibility of access to a separate interface providing
control over the processing of her personal data, in particular as regards the right of access to
personal data or the right to rectification. On the operator's website they can
guidelines and templates for applications for the exercise of the rights of data subjects should be published.
The result should be the processing of applications in the time and in the declared quality.

**19. The operator keeps records of processing activities**
**and ensures that they are kept up to date.** Keeping a record sheet, special
registration and notification obligation is replaced by uniform record keeping of
processing activities that both the **operator** and the
**broker** . Part of the compilation of records of processing activities
There is also a revision of the rights to access individual repositories and an evaluation of their status from
from a security perspective.



**20. Assess whether it applies to the operator or intermediary**
**obligatory obligation to designate a responsible person** - possibly consider the need
and the benefits of the voluntary designation and to demonstrate the fulfillment of its qualifications
assumptions. The roles of the responsible person will be determined.

**21. Data retention period and archiving period** - in accordance with accepted
registry regulations and according to the deadlines set by a special law.

**22. Risk analysis** - each **operator and intermediary is obliged** to comply
with the requirements of Art. 32 Regulations / § 39 of Act no. 18/2018 **Coll. and materials** to which
the output is the adoption of appropriate technical and organizational measures, is necessary
assess the risks and impacts on all their **processing activities** as well as on rights
and freedoms of natural persons. It can already be a useful basis at present
developed security project, if it meets the requirements of legislation.

**Safety project DO NOT DISPOSE! Impact assessment at Safety project!**

**23. Take appropriate security measures**

a) **Technical measures** - e.g. securing the object using mechanical
means of restraint (lockable doors, windows, gilles), a.k.
storage of physical media of personal data documents
in a locked cabinet, protection against damage to
media of personal data by document shredding equipment, rules
third party access to personal data, identification, authentication and
authorization of persons, use of logos, firewall, protection against threats
originating from a publicly accessible computer network (eg a hacker attack),
rules for downloading files from a publicly accessible computer network, protection
against spam, backups, etc.

Regulation / Act no. 18/2018 Coll. defines some security
measures: anonymization, encryption, pseudonymization by the operator
it may **voluntarily** introduce into its processes.

b) **Organizational measures** - education, determination of instructions, which is a person
obliged to apply in the processing of personal data, the definition of personal
data, the definition of the rules for the transfer of personal data, the degree of performing his or her
duties or tasks, managing passwords, controlling access to the object and protected
premises of the operator (eg through technical and technical
personnel measures), the regime of maintenance and cleaning of protected areas,
rules for processing personal data outside the protected area,
handling and protection of business mobile phones, laptops, use
e-mails only for work purposes, the control activity of the operator focused
to comply with the security measures taken, specifying the method, form



and periodicity of its implementation, informing the persons concerned about the control
mechanism, if implemented by the operator (scope of control and methods of control)
implementation.

**24. Risk monitoring.** Operators must constantly assess the risks that
arise as a result of their processing activities, as personal processing
data is a living mechanism. Once security measures are taken, it is required
testing and evaluation, e.g. in the form of penetration tests or other testing
measures taken . Regular updates and optimizations are required.

**25. Document the implementation of the personal data protection policy** . It's not
a mandatory document, but it is a document that demonstrates compliance
the controller is responsible for complying with the principles at the same time
the operator must be able to demonstrate this compliance at any time. On the
Demonstrating compliance with the new legislation may serve to comply with the approved
code of conduct, compliance with the certification mechanism, records
on processing activities, but also, for example, documents on the
implementation of data protection and security policy. Complexity of documentation
depends on the circumstances and risk of the particular processing.

**26. Data protection impact assessment.** According to Art. 35 par. 1 of the Regulations / § 42 par.
1 of Act no. 18/2018 Coll. is **each operator** shall carry out a legal analysis
with a reference to the identification of those **processing operations** for which
presumption that they lead to a **high risk** to the rights and freedoms of individuals. if
each processing operations are identified by the operator only if he is alleged
proceed with the conclusion that **no impact assessment** - the operator will do it
defined in Art. 35 par. 7 of the Regulations / § 42 par. 4 of Act no. 18/2018 Coll., And what
the operator must do in the case of the processing operations for which it is required
Z. z. gives several examples where the processing operation will lead to a high
risk and an impact assessment will be required. It is also necessary to present from the decree
which will include a calculation of the processing operations for which it will be issued
it is necessary to prepare an impact assessment of the so-called blacklist of processing operations .

**27. Prior consultation** - is mandatory before the actual processing begins .
only if the impact assessment shows that the residual "residual" risk of processing on
rights and freedoms of natural persons, even after security measures have been taken against them
mitigation remains high.
The aim of the previous consultation is only a guideline or a proposal for possible ones
other measures, not to obtain the consent / authorization of the processing authority
Responsibility for processing remains with the controller.

**28. Incident management**

Introduce:



- the procedure for reporting security incidents and identified vulnerabilities
places for the purpose of taking preventive or corrective measures in good time
- records of security incidents and solutions used
- identification (by notification or monitoring) and disposal
consequences of security incidents
- Incident analysis: to assess whether or not a security incident is
a breach of personal data protection and personal data protection
the obligation to notify the Office in the event of a breach of protection
personal data within 72 hours.
- notification obligation towards the persons concerned - without undue delay, if
a high risk to the rights and freedoms of the persons concerned shall be assessed.
- implementation of corrective measures
- restoring the availability of personal data (backup is therefore effective)
prevention.

**29. I perform cross-border processing but transfer personal data to third parties**
**countries?** Free movement of personal data between the Slovak Republic and members
guaranteed by EU Member States; basic precondition for the processing of personal data by
any processing operation with personal data, both within and outside the EU
compliance with the principle of legality, as it must be based on legal
on the basis of Art. 6 par. 1 Regulations / § 13 par. 1 of Act no. 18/2018 Coll.

**30. Voluntary possibility of certification, accreditation, introduction of a code of conduct**

CAUTION: This procedure is not universally applicable. It depends on the complexity
individual processes and the volume of personal data processed.

The material is not legally binding, it is only of a recommendatory nature as the environment
each operator or intermediary is unique and requires consideration
specific decisions.