Raczkowski

ul. Chłodna 51 – 00-867 Warszawa – Polska
T +48 22 380 42 50 | F +48 22 380 42 51
office@raczkowski.eu

PERSONAL DATA PROTECTION POLICY AT RACZKOWSKI SP.K.

Warsaw, 1 September 2018

Contents

Purpose 3
Scope of the Policy 3
Definitions 4
General principles of personal data processing 4
Professional confidentiality 5
Security of personal data 5
Principles for processing personal data in traditional form 6
Procedures to be followed in case of a breach of data protection principles ... 7
Rights of data subjects 9
Liability for breaches of personal data processing principles 9
Final provisions 9

PERSONAL DATA PROTECTION POLICY

Purpose

The personal data protection policy ("**the Policy**") has been developed and implemented in order to ensure that in Raczkowski Law Firm ("**the Law Firm**", "**Data Controller**") personal data are:

- processed in accordance with the requirements of the applicable law, i.e. the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of the natural persons with regard to the processing of personal data and on the free movement of such data, and repealing the Directive 95/46/EC ("**GDPR**") and the Act of 10 May 2018 on the Protection of Personal Data (Law Digest of 2018 item 1000), and
- properly safeguarded against the access of unauthorised persons and against accidental loss.

Scope of the Policy

1. The Policy regulates:

a) the principles of processing personal data in the Law Firm,

b) how professional confidentiality is maintained when processing personal data in the Law Firm,

c) the procedures to be followed in case of a breach of data protection principles in the Law Firm,

d) liability for the application and breach of the Policy.

2. IT security is regulated in a separate document.

3. The Policy concerns all actions related to the processing of personal data processed irrespective of the type of data, their source, and manner of processing, including in particular:

a) personal data obtained in connection with providing legal assistance by the Law Firm,

b) personal data of persons employed at the Law Firm or co-operating with the Law Firm irrespective of the type of the legal relationship between these persons and the Firm (in particular, including on the basis of the employment relationship, civil law agreement, trainees and interns) and applicants.

c) personal data of persons in permanent legal relations with the Law Firm in connection with the business of the Law Firm,

d) personal data of persons participating in the events organised by the Law Firm,

e) personal data of subscribers of the publications of the Law Firm,

4. The Policy applies to any person who processes personal data in the Law Firm irrespective of the legal basis of the relationship between such person and the Law Firm.

Definitions

a) **Data Controller** – Raczkowski Law Firm with its registered office in Warsaw, ul. Chłodna 51, 00-867 Warszawa, entered into the register of entrepreneurs of the National Court Register under number: 0000373899;

b) **personal data** – any information relating to an identified or identifiable natural person (a data subject), in particular on the basis of the first name and surname, but also on the basis of location data or online identifier;

c) **data subject** – any natural person whose personal data are processed by the Law Firm;

d) **authorised person** – any natural person who processes personal data in the scope and for the purpose specified in the agreement made with the Law Firm, on the basis of a personal authorisation to process data granted by the Data Controller;

e) **data processing** - any operation or a set of operations performed on personal data or sets of personal data, whether or not by automated means, such as: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

f) **professional confidentiality** – confidentiality defined in Article 6 of the Act of 26 May 1982 the Law on the Bar (Law Digest 2018.1184), Article 3 of the Act of 6 July 1982 on Attorneys-at-Law (Law Digest 2017.1870) and Article 37 of the Tax Advisory Act of 5 July 1996 (Law Digest 2018.337).

General principles of personal data processing

5. The Law Firm processes personal data in connection with its business activity in accordance with the applicable laws.

6. The Law Firm maintains a register of data processing operations.

7. The Law Firms may entrust certain personal data processing activities to an entity not operating within the Law Firm, whilst ensuring the compliance with the principles of professional confidentiality. In such cases, the Law Firm shall enter into a data processing agreement with such an entity which meets the legal requirements set out in Article 28 of the GDPR.

8. The Law Firm does not transfer personal data processed by it to third countries or international organisations within the meaning of Article 4(26) of the GDPR.

9. Personal data are processed in accordance with the principles of processing, which means that personal data are:

   a) processed only where at least one legal basis for data processing provided for by the law applies,

   b) processed fairly and in a transparent way in relation to the data subjects, subject to restrictions resulting from the obligation to maintain professional confidentiality,

   c) collected for specified, clear, and legitimate purposes and not further processed in a manner incompatible with these purposes;

d) adequate, relevant, and limited to what is necessary for the purposes for which they are processed,

e) accurate and, where necessary, kept up to date;

f) stored in a form which permits identification of the data subject for the period no longer that it is necessary for the purposes for which the data are processed,

g) processed in a manner that ensures appropriate security, including protection against unauthorised or illegal processing and accidental loss, destruction or damage, using appropriate technical or organisational measures.

10. The Data Controller shall take all reasonable actions in order to ensure that personal data that are inaccurate in the light of the purposes for which they are processed, are erased or rectified without delay.

11. An information clause for persons designated for contact or representing the Client must be attached to the cooperation agreement between the Law Firm and the Client which is tantamount to fulfilling the obligations referred to in Articles 13 and 14 of the GDPR.

Professional confidentiality

12. Notwithstanding the principles set out in the personal data protection regulations, personal data processed in connection with providing legal assistance are covered by professional confidentiality.
13. Professional confidentiality covers all information, messages, notes, and documents concerning a case obtained in relation to the case, including those obtained from the Client or other persons irrespective of the place where they are located and the form they were recorded in.
14. Persons cooperating within the Law Firm with an advocate, attorney-at-law or tax advisor are obliged to maintain confidentiality in matters covered by their professional confidentiality.
15. Persons who are not advocates, trainee advocates, attorneys-at-law, trainee attorneys-at-law, tax advisors submit written declarations undertaking to maintain confidentiality during the processing of the data and after its completion (without any time limit) to an extent no less than that to which professional confidentiality binds an advocate, attorney-at-law or tax advisor.

Security of personal data

16. The Law Firm uses organisational and technical measures in order to ensure that all operations on personal data are carried out with due regard for the rights and freedoms of the data subjects.
17. The authorised person having access to personal data, processes such data only on the instructions of the Data Controller, unless the provisions of law require it.

18. The authorised person is required in particular to:

a) observe the scope of their authorisation,

b) process and protect personal data in accordance with the applicable regulations of the general law, internal documents of the Data Controller, and the Policy,

c) maintain the confidentiality of personal data and measures of their protection also after the termination of the legal relation between them and the Law Firm,

d) immediately report any suspected breach of the principles of personal data protection to the following email address specifically created for this purpose: rodo@raczkowski.eu.

19. The Law Firm, either at its own initiative or at the request of an authorised person, provides information, advice, and guidelines concerning the manner in which the personal data processing should be carried out.

20. Personal data are processed in the Law Firm – in its registered office and local branches, i.e. in the office premises in the following locations:

- in Warsaw - ul. Chłodna 51 (the Law Firm's registered office),
- in Cracow - ul. Krupnicza 16 (a regional office),
- in Poznań - ul. Mielżyńskiego 14 (a regional office).

The access to the office premises is secured against unauthorised entry. Outside working hours the office premises are secured by an alarm system or monitored by security staff of the building in which they are located.

21. If it is necessary to carry out the activities outside the Law Firm, in particular during business trips, online work etc. the authorised person is obliged to take the utmost care to ensure data confidentiality, in particular:

a) to ensure that the place in which they are located provides appropriate conditions for the security of information during work (in particular, it should be considered whether it is possible to work on public transport whilst ensuring confidentiality),

b) not to leave files, documents, notes etc. unattended,

c) to refrain from using personal data or Client names during telephone conversations held in public places and on public transport.

Principles for processing personal data in traditional form

Processing of personal data in traditional (paper based) form shall be carried out in compliance with the following principles:

a) during work only the documents and notes necessary for work on the day shall be placed on the desk,

b) the authorised person is responsible for all copies and print-outs containing personal data which they have made and for ensuring that they are properly secured; any surplus documents which may be made in exceptional situations must be destroyed at the end of the working day; before printing or copying a document containing personal data it should be assessed what number of copies is necessary for the purpose,

c) when leaving the workplace after finishing work for the day, the authorised person must not leave any documents or notes containing personal data on the desk or in any other visible place which has not been designated by the Data Controller for storing documentation,
d) documents or notes containing personal data, in particular files of court cases, shall be stored exclusively in specially designated places, in locked cabinets and shall be marked as confidential,
e) after the working day the keys to the cabinets shall be properly secured, in particular they cannot be left in any visible place,
f) authorised persons processing personal data as part of criminal law and compliance practice, personal data protection practice, and employee taxes practice, must comply with the enhanced personal data protection principles set out by the Partner responsible for the relevant practice,
g) original documents containing personal data should be properly secured against their accidental loss, damage or destruction. In particular:
- one should exercise caution when making copies or scans of documents so that they are not left in the device used for copying or scanning,
- original documents should not be left unattended by an authorised person,

h) original documents should only be used to the extent necessary to perform a given action and when it is completed they should not be stored in the Law Firm, unless the period of their storage was agreed with the Client,
i) documents with respect to which there is no justified need for constant access, in particular after the conclusion of the case or provision of service, should be archived if they are subject to archiving. Otherwise, in consultation with the person responsible for the case, they should be anonymised or returned to the Client.

Procedures to be followed in case of a breach of data protection principles

22. The authorised person is obliged to take remedial measures on an ongoing basis, in particular those specified in the Policy, in order to prevent any breach of personal data protection.

23. A breach of personal data protection is defined as a security breach leading to an accidental, unlawful destruction, loss, alteration, unauthorised disclosure or unauthorised access to personal data transmitted, stored or otherwise processed.

24. A breach of personal data protection includes in particular the following:

a) a loss (theft, misplacement) of a laptop, telephone, portable hard drive, bag or file containing personal data,

b) leaving documents containing personal data in a place accessible to unauthorised persons,

c) a breach of confidentiality, access or unauthorised alteration of data content,

d) the condition of rooms and cabinets, or office furniture in which documentation is stored or the contents of the documentation which give rise to suspicions that third parties may have accessed them,

e) incorrect addressing of electronic mail or failing to use the “blind carbon copy” option, i.e. not concealing individual recipients of the message.

25. In the event of a personal data protection breach or in the event of an attempted or suspected breach, a person aware of such an incident is obliged to immediately notify the Partner responsible for personal data protection and the Partner responsible for IT by phone and by email by sending a message to the following address: rodo@raczkowski.eu.
26. Irrespective of the above, the authorised person is obliged to take all appropriate actions which in these circumstances should be taken in order to limit the negative impact of the incident, provided that such actions are obvious and do not require consultation with the Partner or the IT department.
27. In the event of establishing that a personal data protection breach has occurred, which is likely to result in a risk of breach of rights or freedoms of natural persons in the extent confirmed by the Partner responsible for personal data protection and the Partner responsible for IT, the Law Firm is obliged to notify the President of the Office for Personal Data Protection of this fact without undue delay – if possible within 72 hours of receiving confirmed information about the breach.
28. If in the opinion of the Data Controller it is unlikely that the personal data protection breach should result in a risk of breach of rights or freedoms of natural persons, the President of the Office for Personal Data Protection shall not be informed about the breach, however the breach shall be recorded in the register of breaches, together with reasons for this.
29. If the breach of personal data protection may result in a high risk of breach in rights and freedoms of natural persons, the Law Firm notifies the data subject about the breach without undue delay.
30. The notification referred to in point 27 above is not required if:

a) the Data Controller has implemented appropriate technical and organisational security measures and these measures have been applied to the personal data affected by the breach, in particular such measures as encryption, which prevent unauthorised persons from accessing these personal data;

b) the Data Controller has then applied measures eliminating the likelihood of high risk of breaching of rights or freedoms of a data subject referred to in point 22;

c) it would require a disproportionate effort. In this case a public communication is released or a similar measure is applied to inform the data subjects in an equally effective manner.

31. In the event referred to in point 27, information regarding the notification of the data subject or, where applicable, the reasons for not providing such notification is placed in the register of breaches.
32. The Law Firm maintains an electronic register of all personal data protection breaches, irrespective of whether they were subject to notification referred to above.

Rights of data subjects

33. If in connection with the processing of personal data by the Law Firm, a data subject expresses their intention to exercise any of the data subject rights referred to in Chapter III of the GDPR, the Data Controller shall take a decision on the scope in which this request is to be granted, taking into account the restrictions resulting from the obligation to maintain professional confidentiality.
34. If the request of the data subject is made to the authorised person, that person shall immediately notify the Partner responsible for personal data protection in the Law Firm.

Liability for breaches of personal data processing principles

35. Persons processing personal data may be held liable for a breach in the principles of personal data processing on the conditions specified in the provisions of generally applicable law.
36. A breach in the principles of personal data protection may be:

a) grounds for the termination of an employment agreement and in case of conduct constituting a serious breach of employee obligations, termination without notice.

b) a valid reason for terminating a service agreement.

Final provisions

37. The Policy was made in writing in one copy kept by the Executive Director.
38. The electronic version of the Policy has been made available by placing it in the Intranet of the Data Controller.
39. The Policy becomes effective on 1 September 2018.
40. At least once every calendar year, the Partner responsible for personal data protection shall review the regulations contained in the Policy in order to verify their adequacy for the type and degree of risk related to personal data processing, in order to limit this risk.

How to contact the Data Controller: the Data Controller may be contacted by sending a message to the following email address: rodo@raczkowski.eu or by writing to the address of the registered office of the Data Controller.