



CODE OF CONDUCT PROCESSING PERSONAL DATA
iPS Holding B.V. and/or its affiliated companies

Contents

CONSIDERATIONS	3
PARAGRAPH 1: GENERAL PROVISIONS	3
Art. 1: Definitions	3
PARAGRAPH 2: PRINCIPLES OF DATA PROCESSING	4
Art. 2: Scope and principles for processing personal data	4
Art. 3: Purpose for data processing	4
Art. 4: Provision of data	5
Art. 5: Processing of personal data	5
Art. 6: Special data	7
Art. 7: What if the recipient does not provide personal data to the controller?	8
Art. 8: Retention period	8
PARAGRAPH 3: PROVISION OF DATA	9
Art.9: Provision of data to recipients	9
Art. 10: Provision of data to processors	9
Art. 11: Compatible use	9
Art. 12: International Aspects	9
PARAGRAPH 4: INFORMATION OBLIGATION, ACCESS AND CORRECTION	10
Art. 13: Information obligation	10
Art. 14: Right of access to the person concerned	10
Art. 15: Improvement, replacement, deleting or blocking	10
PARAGRAPH 5: SECURITY AND CONFIDENTIALITY	11
Art. 16: Security and protection of personal data	11
Art. 17: Confidentiality	11
PARAGRAPH 6: FINAL PROVISION	11
Art. 18: Lodging a complaint	11
Art. 19: Changes to this privacy statement	11
Art. 20: Contact	12

CONSIDERATIONS

iPS Holding B.V. and/or its affiliated companies (hereinafter referred to as the controller), takes into consideration that:

- the General Data Protection Regulation (GDPR) sets rules for the protection of personal data;
- the General Data Protection Regulation (GDPR) is aimed at setting guarantees to protect the fundamental rights and freedoms, in particular, the protecting of privacy;
- article 40 of the General Data Protection Regulation (GDPR) offers the controller the possibility, given the characteristics of the sector in which it operates, to draft such a Code of Conduct that is an elaboration of this act or to other legal provisions regarding the processing of personal data;
- the controller processes personal data of natural persons, within the framework of its normal business operations, and takes into consideration the importance to process personal data with great care;
- the controller provides full disclosure to maximise a complete transparency for all persons concerned.

has taken into regard:

- the General Data Protection Regulation (Regulation Data Protection Regulation (EU) 2016/679);

decided to be bound by the following Code of Conduct.

PARAGRAPH 1: GENERAL PROVISIONS

Art. 1: Definitions

In the context of this Code of Conduct the definitions hereunder shall have the following meaning;

- the GDPR:** General Data Protection Regulation (Regulation Data Protection Regulation (EU) 2016/679);
- personal data:** any information concerning an identified or identifiable natural person;
- processing of personal data:** any action or any set of operations concerning personal data including the collection, recording, ordering, storage, adoption or alteration, retrieval, consultation, use, dissemination by means of transmission, distributing or making available in any other form, merging, linking, as well as blocking, deleting or destructing of data;
- file:** any structured set of personal data that is accessible according to specific criteria and related to (different) natural persons, whether centralised, decentralised or dispersed in a functional or geographical manner;
- controller:** iPS Holding B.V. and/or its affiliated companies, which determines the purpose and means of processing personal data;
- processor:** the person or company that processes personal data for the controller without falling under its direct authority;
- person concerned:** the person to whom an item of personal data relates to;

- h. **third party:** every other person, not being the person concerned, the controller, the processor or any person who is falling under the direct authority of the controller or the processor and is authorised to process personal data;
- i. **recipient:** a person or organisation to whom personal data will be provided, being the client or a (government) agency;
- j. **third country:** a country located outside the European Economic Area;
- k. **Dutch Data Protection Authority:** the supervisor as mentioned in Article 51, paragraph 1 GDPR;
- l. **providing personal data:** the revealing or providing of personal data;
- m. **collection of personal data:** obtaining personal data.

PARAGRAPH 2: PRINCIPLES OF DATA PROCESSING

Art. 2: Scope and principles for processing personal data

1. This Code of Conduct is applicable to any form of processing of personal data by the controller, the authorised staff of the controller, or any processor hired by the controller.
2. The controller processes personal data exclusively in accordance with the six principles of the GDPR ('accountability'):
 1. Lawful, fair and transparent;
 2. Purpose limitation;
 3. Data minimisation;
 4. Accuracy;
 5. Storage limitation;
 6. Integrity and confidentiality.
3. Personal data shall only be processed if:
 - a. the person concerned has given his unambiguous consent to the controller for the processing of personal data;
 - b. the data processing is necessary for the execution of an agreement to which the person concerned is a party, or for taking pre-contractual measures that are necessary to conclude such an agreement;
 - c. the processing is necessary in order to fulfil a legal obligation to which the controller or the recipient is subjected to;
 - d. the processing of personal data is necessary in order to protect the vital interests of the person concerned; or
 - e. the processing of personal data is necessary for the purpose of the legitimate interests pursued by the controller or a third party to whom the data is disclosed, unless the interest or fundamental rights and freedoms of the person concerned, in particular, the right to privacy, prevails. The processing will be ended if the interest of the person concerned prevails.

Art. 3: Purpose for data processing

1. The controller processes personal data for the purpose of obtaining or providing information concerning natural persons, to support the preparation and/or settlement of the decisions that must be taken by the controller and/or recipients concerning:
 - a. the selection of (potential) candidates;
 - b. the entering or termination of any employment relationship;
 - c. whether or not to apply, respectively continue assignments and/or agreements;
 - d. determining the conditions under which assignments and/or agreements take place;
 - e. whether or not to enter into rights and obligations that are necessary for the context of the implementation of assignments and/or agreements.
 - f. the termination of assignments and/or agreements;
 - g. determining rights and obligations that stem from (legal) obligations and regulations.
 - h. entering into such rights and obligations.
2. Taken into account the provisions of Article 2 of this Code of Conduct, the aforementioned purposes listed here provide the legitimate base for the processing of personal data.

Art. 4: Provision of data

1. Taken into account the principles of diligence and carefulness, the processed personal data can derive from:
 - a. the person concerned or on his behalf; if personal data will be obtained by a third party on behalf of the person concerned, the controller should ensure that this third party is authorized or otherwise competent to obtain the data on behalf of the person concerned, unless the competence can reasonably be presumed;
 - b. a third party who maintains or has maintained a financial or business relationship for the respective particular processing purpose with the person concerned and who has obtained this data within the framework of the purpose of the processing, insofar as obtaining of the data is not incompatible with the purpose for which it was collected;
 - c. a third party that maintain or has maintained an employment relationship with the person concerned;
 - d. public registers, such as the Trade Registry of the Chamber of Commerce; Land Registry, the Central Register of Insolvencies; Receivership Register;
 - e. public sources and registers, such as Registries of Subdistrict Courts (bankruptcies, suspensions of payments, debt restructuring); the Dutch State Gazette (Staatscourant); internet;
 - f. public document verification- and signaling registers;
 - g. international equivalents of the sources mentioned above.
2. Personal data will be processed in such a manner that expresses the nature of the source from which it is obtained.

Art. 5: Processing of personal data

1. Personal data shall only be processed insofar as it is sufficient, relevant and not excessive given the purpose for which it was collected or for which it was processed.

2. The following types of personal data can be processed:
 - a. name, address, zip code, residence, date of birth or age, place of birth or native country, gender, marital status, family status, BSN and/or passport number, telephone number, email address and/or other relevant data for identification and communication;
 - b. names of present and former employer(s);
 - c. data relating to training and certificates;
 - d. court decisions such as attachment under an execution, summons or notification of judgements;
 - e. juridical decisions regarding bankruptcy, suspension of payment and debt restructuring due to the Dutch and/or foreign legislation, such as the Natural Persons Composition Act;
 - f. the start and end dates of your employment or appointment;
 - g. your family members and their contact details;
 - h. appointment file, including personal information contained in a CV, application forms, accompanying letters, interview notes, references, copies of work permits, copies of diplomas/certificates, copies of driving licences and other documents for background checks;
 - i. the terms and conditions of your employment or appointment (including your position and working hours), as set out in a letter of offer, employment contract, confirmation of appointment, temporary worker agreement, consultancy agreement, letters regarding salary increases and bonuses, statements of changes to the terms and conditions of employment or appointment, and related correspondence;
 - j. details of your skills, qualifications, experience and employment history, both with previous employers and within the employer;
 - k. memberships of professional organisations;
 - l. your salary and entitlement to benefits/pensions;
 - m. your national insurance number;
 - n. your bank details, payroll records, tax rate group and other tax information;
 - o. any information about disciplinary measures, complaints and suitability, including investigation reports, collected evidence, minutes of hearings and appeal hearings, warning letters, performance improvement plans and related correspondence;
 - p. assessments, including assessment forms, performance assessments and ratings, targets and goals set;
 - q. overview of training/education courses attended;
 - r. data on holiday and other forms of leave, including details of the type and reason for taking leave and related correspondence;
 - s. documentation relating to the termination of employment or appointment, including letters of dismissal, notices, minutes of meetings, settlement agreements and related correspondence;
 - t. information obtained electronically, such as swipe card or time card data;
 - u. information about training/education courses attended;
 - v. information about your use of our IT systems, including the use of telephones, email and the internet;
 - w. access card log data for the building;
 - x. photographs;
 - y. camera images (e.g. for security or promotional material);
 - z. login details for various accounts that are or have been used by employees on behalf of;
 - aa. certificate of good conduct (VOG);
 - bb. other data necessary for the purpose of processing.
3. The controller shall take all the necessary provisions to promote the accuracy and completeness of the processed personal data.
4. If there is a reasonable suspicion that the personal data is not accurate anymore, the controller should examine the accuracy of the data and if necessary improve, supplement, remove or block such data.
5. In offering its services, the controller uses a server park that is located in the Netherlands. Consequently, Dutch law and regulations are applicable to the processing of personal data. This server park is managed and maintained by the controller and a processor with whom the controller has concluded a Service Level Agreement and a Data Processing Agreement. All the activities will be maintained in an administration that is carried out by the controller.

Art. 6: Special data

1. No personal data will be processed concerning someone's religion or belief, race, political opinion, health and sexual orientation, as well as a trade-union membership.
2. The provisions of the first paragraph are not applicable;
 - a. if the data is processed with the explicit permission of the person concerned;
 - b. if the data is manifestly made public by the person concerned;
 - c. if the processing regards data concerning race that is inevitable in order to contribute to the identification of the person concerned;
 - d. if this is done with a view to monitoring equal opportunities and in accordance with data protection policy. Personal data used by the controller for these purposes shall be anonymised or collected with explicit written consent, which may be withdrawn at any time. It is entirely up to the data subject to provide such personal data.
 - e. insofar as the data is necessary for:
 - i. an adequate application of (foreign) statutory regulations, which include the obtaining of required permits or the implementation of pension schemes or collective labor agreements that provide in entitlements that are dependent on the health status of the person concerned; or
 - ii. the reintegration, guidance or support of employees or benefit recipients in connection with illness or incapacity for work. This may therefore involve information about the employee's health, including medical conditions, whether there is a disability for which the controller must make reasonable adjustments, sick leave records (including details of the reasons for sick leave), medical reports and related correspondence. The above only applies if and insofar as the employee has given consent to share the aforementioned medical information with the controller.
 - f. Certain special categories of personal data, namely information about the employee's health or medical conditions and trade union membership, information about criminal convictions and offences, are processed so that the controller can fulfil its obligations or exercise its rights under labour law or social security law, in accordance with data protection policy. Information about health status or medical conditions may also be processed to assess an employee's fitness for work or medical diagnosis, provided that this is done under the responsibility of a medical professional bound by professional secrecy, such as a doctor, and again in accordance with data protection policy.
 - g. in all the other cases permitted by the GDPR.
3. Data of a criminal or disciplinary nature shall not be processed. Therefrom is excluded data concerning financial-economic crimes insofar as the data comes from open sources and insofar as the documentation is necessary for a responsible practice by the controller. Criminal convictions and offences are also excluded, where permitted by law and relevant to the position. These special categories of personal data and information about any criminal convictions and offences are or will be processed for the following purposes:
 - a. Assessing suitability for a position, appointment or promotion;
 - b. Complying with legal and/or regulatory requirements and obligations, such as conducting criminal record checks;
 - c. Complying with the obligation to make reasonable adjustments for employees and workers with disabilities, and other obligations to prevent discrimination on the basis of disability;
 - d. Managing and maintaining a register for sick leave procedures;
 - e. Determining fitness for work;
 - f. Managing, planning and organising work;
 - g. Effective personnel management;
 - h. Ensuring the payment of sick pay;
 - i. Complying with our obligations under health and safety legislation;
 - j. Making decisions about the continuation of an employment contract or appointment;

- k. Managing and maintaining a register for dismissal procedures;
- l. Maintaining effective general HR, personnel and business administration;
- m. Ensuring compliance with company regulations, policies and procedures;
- n. Monitoring equal opportunities;
- o. Payment of trade union dues;

Art. 7: What if the recipient does not provide personal data to the controller?

1. One of the reasons for processing personal data is to enable the controller to perform its tasks as set out in the employment contract or any other agreement. If the data required for this purpose is not provided in whole or in part, the controller will not be able to perform those tasks. For example, ensuring that salary payments are made correctly, the controller needs the correct bank account number. The controller may also be prevented by legal obligations from confirming or continuing the employment relationship if the data subject does not provide relevant information. This concerns, for example, confirming immigration status and the right to work in a country or, where applicable, confirming the legal status to perform work via a criminal record check (VOG).

Art. 8: Retention period

1. Personal data shall be stored for the period that is necessary regarding the purpose of the processing. The controller generally retains personal data for the duration of the employment or appointment. The following exceptions apply:
 - a. Personal information provided as part of the application process will not be retained if it is not relevant to the current employment relationship;
 - b. Personal information about criminal convictions and offences collected during the application process will be destroyed once it has been verified by means of a criminal record check, unless the information has been assessed by the controller as relevant to the current employment relationship;
 - c. A criminal record check is destroyed as soon as the conviction has expired (unless information about expired convictions can be retained because the position is an excluded profession or occupational group); Data on disciplinary measures, complaints and suitability are only kept until the expiry date of a warning (however, a summary of the disciplinary measure, complaint or performance management system is kept for the duration of your employment).
2. Once employment has ended, personal data is generally retained for up to two years after termination of employment, but this depends on:
 - a. the minimum legal or other statutory, tax, health and safety, reporting or accounting requirements for specific data or records, and
 - b. the retention of certain types of personal data for up to six years as protection against legal risks, for example if they could be relevant to a possible legal claim.
3. The controller will keep payroll and tax records (including information about salary, bonuses, overtime, expenses, benefits and pension, national insurance number, income tax records, tax rate group and other tax data) for up to 7 years after termination of employment. All in all, this means that the personal data file will be thinned out two years after the termination of employment, so that only the strictly necessary data will be retained for a longer period of time.
4. Personal data that no longer needs to be retained will be destroyed or permanently deleted from our IT systems in a secure and effective manner, and the controller will also require third parties to destroy or delete such personal data, if applicable.
5. In some cases, personal data will be anonymised so that the data subject can no longer be identified. In that case, the controller will retain such information for a longer period.

PARAGRAPH 3: PROVISION OF DATA

Art.9: Provision of data to recipients

1. All personal data that the controller provides orally, written, through data communication or data carriers, regardless of the layout and whether or not in compressed formats, to a recipient as a result of automatic processing, will only be provided at prior request of such a recipient and in accordance with the purpose mentioned in Article 3.
2. Provision to recipients does not take place if the controller knows or has reasonable grounds to believe that the data:
 - a. shall be published or utilised in a wider circle;
 - b. will be used for purposes that are not in line with the purpose of the processing.
3. If there is a reasonable suspicion that the personal data is no longer up to date, provision thereof shall only take place after the data has been examined on accuracy.

Art. 10: Provision of data to processors

1. If the controller processes personal data by means of a processor on its own behalf, it shall ensure that sufficient guarantees regarding technical and organisational security measures for such processing operations are offered. The controller shall also supervise the compliance of these measures.
2. The carrying out of a processing operation by way of a processor shall be governed by an agreement or another legal act whereby a commitment arises between the processor and the controller.
3. The controller shall ensure that the processor:
 - a. only processes the personal data in accordance with the controller's mandate;
 - b. keeps the personal data confidential;
 - c. fulfils the obligations of the controller that are derived from Paragraph 4 of this Code of Conduct.
4. If the processor is located in another country of the European Economic Area, the controller shall ensure that the processor fulfils its duties under the law of that other country, in derogation from Article 9 section 3 subsection c of this Code of Conduct.

Art. 11: Compatible use

1. Personal data is obtained for the legitimate purposes mentioned in Article 3 and may not be processed further in a way that is incompatible with these purposes.
2. In determining whether there is compatible use, the controller shall take into account the relationship between the purpose of the intended processing and the purpose for which the data is obtained, the nature of the respective data, the consequences of the intended processing for the person concerned, the manner in which the data is provided and the extent wherein appropriate guarantees are foreseen towards the person concerned.

Art. 12: International Aspects

1. This Code of Conduct is also applicable to the processing of personal data in a third country if the controller is located in the Netherlands.

2. The controller only gives personal data, that is subjected to provision or is intended for provision after transfer, to a recipient or processor from a third country if an adequate level of protection is guaranteed or if one of the exceptions in Chapter 5 of the GDPR is applicable.

PARAGRAPH 4: INFORMATION OBLIGATION, ACCESS AND CORRECTION

Art. 13: Information obligation

1. In the case of automated processing or manual processing of personal data in a document, the controller shall inform the person concerned about its identity and the purpose of the processing:
 - a. if personal data is obtained from the person concerned, before or at the time of the acquisition;
 - b. if personal data is obtained in a different manner:
 - i. at the moment of the registration;
 - ii. no later than the moment of the first provision, when the data is intended to be disclosed to a recipient, unless the controller can assume on substantial grounds that the person concerned is already informed.
2. The obligation, as referred to in the first section, can be discarded if this is necessary for the interest of others than the person concerned, the controller included therein. In that case, the controller establishes the source of the data.

Art. 14: Right of access to the person concerned

1. Within four weeks, the controller shall inform anyone in writing, at their own request and after determination of their identity, whether personal data concerning them has been processed or not. If the personal data is requested for by another person than the person concerned, the controller must ensure that the applicant is authorised or is otherwise entitled to request this personal data on behalf of the person concerned, unless such entitlement can reasonably be presumed.
2. If such data shall be processed, a complete written overview of all the processed personal data shall be provided to the applicant at request within four weeks, along with intelligence regarding the nature of the sources from which the data is derived. In addition, a description of the purpose and objectives will be submitted, as well as information concerning the personal data and recipients.
3. The obligations as mentioned in this Article can be set aside insofar as this is necessary for the interests of others than the applicant, the controller included therein.

Art. 15: Improvement, replacement, deleting or blocking

1. Following a message, respectively a request thereto from the person concerned, the controller shall correct, supplement, delete or block the personal data that is factually inaccurate, incomplete, or is processed in conflict with a statutory regulation or the purpose of the processing, as soon as possible after the discovery thereof.
2. In the case the information provided by the person concerned and/or the explanation thereof, in the opinion of the controller, forms an insufficient ground for immediately correcting, supplementing, deleting or blocking of the data as described in the first section or if this otherwise results in questions regarding the accuracy, respectively the completeness of the processed personal data of the person concerned, the controller will additionally investigate this.

3. The person concerned receives within 4 weeks after submitting a notification, respectively a request as mentioned in the first section, a written notice from the controller about whether or not personal data is corrected, supplemented and/or removed.
4. In case the controller corrects, supplements, deletes or blocks the personal data as a result of a notification, respectively a request from the person concerned, as mentioned in the first section, the controller shall inform those to whom the personal data of the person concerned is provided to about any correcting, supplementing, blocking or deleting, unless this is impossible or brings with it a disproportionate effort.

PARAGRAPH 5: SECURITY AND CONFIDENTIALITY

Art. 16: Security and protection of personal data

1. The controller shall implement technical and organisational measures to secure personal data against loss or any form of unlawful processing. Considering the state of the technology and costs of the implementation, these measures shall ensure a level of security appropriate to the risks of the processing and the nature of the data to be protected. These measures are also focused on the unnecessary collection and further processing of personal data. The processor has an equal obligation for the whole or a part of the equipment, which it has in its possession.
2. Within the organisation of the controller, only the representatives that are authorised by the controller shall have exclusive access to the files concerning personal data. The controller will mention all the names of these authorised representatives in a register designated for such a purpose.
3. The controller shall also have procedures in place in the event of a suspected data breach, and the controller shall notify the appropriate supervisory authority or controller and the data subject of a suspected breach where there is a legal obligation to do so.

Art. 17: Confidentiality

1. The authorised representatives are subjected to an obligation of strict confidentiality, unless a legal provision or duty requires them to disclosure.
2. The authorised representatives must state in writing towards the controller that they are made aware of this Code of Conduct and that they shall act in accordance with the provisions thereof.

PARAGRAPH 6: FINAL PROVISION

Art. 18: Lodging a complaint

1. If the recipient believes that their data protection rights have been violated in any way by the controller, they may lodge a complaint with the data protection supervisory authority in the country where they reside. In the Netherlands, this is the Dutch Data Protection Authority ('Autoriteit Persoonsgegevens') via <https://autoriteitpersoonsgegevens.nl/en/submitting-a-tip-off-or-a-complaint-to-the-ap>.

Art. 19: Changes to this privacy statement

1. The controller reserves the right to update or amend this privacy statement at any time, including when the controller intends to further process personal data for a purpose other than that for which the personal data was collected or if new categories of personal data are processed. The controller will publish a new privacy statement when significant updates or changes are made.

2. The controller may also provide information about the processing of personal data in other ways.

Art. 20: Contact

1. This Code of Conduct is available on the controller's website through the following link:
www.ipspowerfulpeople.com/downloads.
2. This Code of Conduct may be sent along with the agreement between the controller and the person concerned. Copies thereof can be ordered via the following e-mail address:
privacy@ipspowerfulpeople.com. For any questions about this code of conduct or the processing of personal data by the controller, please contact us at the above email address.