

Spypoint Personal Information Protection Policy

Last modification: November, 1st, 2018

The Personal Information protection policy (the “**Policy**”) of 9138-4529 QUÉBEC INC., doing business as Spypoint (“**Spypoint**”) is modelled after the principles set out in the national standard of Canada entitled “*Model code for the protection of personal information*” (CAN/CSA-Q830-96) and takes into account provisions of the General Data Protection Regulation of the European Union (“**GDPR**”, entitled “*Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Information and on the free movement of such data, and repealing Directive 95/46/EC*”).

Nothing in this Policy has the effect of creating obligations for Spypoint beyond those imposed by applicable laws and regulations pertaining to protection of Personal Information.

TABLE OF CONTENT

This Policy covers the following aspects of Personal Information protection:

1. Accountability
2. Purposes and Purpose Limitation
3. Consent
4. Limited Collection, Data Minimization, Fairness and Lawfulness
5. Limited Use, Disclosure and Retention
6. Accuracy, Integrity, Confidentiality and Right to Rectification
7. Safeguards
8. Openness and Transparency
9. Individual Access and Other Rights
10. Challenging Compliance

DEFINITIONS

In this Policy:

- Your “**Consent**” means any freely given, specific, informed and unambiguous indication of your wishes by which you, by a statement or by a clear affirmative action, signify agreement to the Processing of Personal Information relating to you.
- “**Controller**” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Information.
- “**Intermediary**” means a natural or legal person, public authority, agency or other body which processes Personal Information on behalf of Spypoint.
- “**Personal Information**” means any information relating to an identified or identifiable natural person and allows that person to be identified.

- **“Personal Information Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Information transmitted, stored or otherwise processed.
- **“Platform”** refers collectively to the websites accessible at www.spypoint.com and www.myspypoint.com.
- **“Processing”** means any operation or set of operations performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **“Profiling”** means any form of automated Processing of Personal Information consisting of the use of Personal Information to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
- **“Pseudonymisation”** means the Processing of Personal Information in such a manner that the Personal Information can no longer be attributed to a specific individual without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Information is not attributed to an identified or identifiable natural person.
- **“Recipient”** means a natural or legal person, public authority, agency or another body, to which the Personal Information is disclosed, whether a third party or not.
- **“Restriction of Processing”** means the marking of stored Personal Information with the aim of limiting its Processing in the future.
- **“Third Party”** means a natural or legal person, public authority, agency or body other than you (as a data subject), Controller, Intermediary and persons who, under the direct authority of Controller or Intermediary, are authorised to process Personal Information.
- **“you”** refers to you or any specific individual as an identified or identifiable natural person.

<h2>SUMMARY OF THE POLICY</h2>

1. **ACCOUNTABILITY:** Spypoint is responsible for, and will be able to demonstrate compliance with this Policy, and has designated an individual or individuals accountable for Spypoint's compliance with the Policy.
2. **PURPOSES AND PURPOSE LIMITATION:** The purposes for which Personal Information is collected will generally be identified by Spypoint at or before the time

the Personal Information is collected, for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3. **CONSENT:** Your knowledge and Consent are required for the Processing of your Personal Information, except where inappropriate.
4. **LIMITED COLLECTION, DATA MINIMIZATION, FAIRNESS AND LAWFULNESS:** The collection of Personal Information will be adequate, relevant and limited to that which is necessary for the purposes identified by Spypoint for which it is processed. Personal Information will be collected by fair and lawful means.
5. **LIMITED USE, DISCLOSURE AND RETENTION:** Personal Information will not be processed for purposes other than those for which it was collected, except with your Consent or as required by law. Personal Information will be retained only as long as necessary for the fulfilment of those purposes in a form which permits your identification for no longer than is necessary for the purposes for which the Personal Information is processed.
6. **ACCURACY, INTEGRITY, CONFIDENTIALITY AND RIGHT TO RECTIFICATION:** Personal Information will be as accurate, complete and kept up-to-date as is necessary for the purposes for which it is to be used. Every reasonable step will be taken to ensure that Personal Information that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.
7. **SAFEGUARDS:** Personal Information will be protected by security safeguards appropriate to the sensitivity of the Personal Information, including protection against unauthorized or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.
8. **OPENNESS AND TRANSPARENCY:** Spypoint will make readily available to you specific information about its policies and practices relating to the management of your Personal Information, which will be processed in a transparent manner.
9. **INDIVIDUAL ACCESS AND OTHER RIGHTS:** Upon request, you will be informed of the existence and Processing of your Personal Information and will be given access to that Personal Information. You will be able to challenge the accuracy and completeness of the Personal Information and have it amended as appropriate.
10. **CHALLENGING COMPLIANCE:** Your Personal Information will be processed lawfully and fairly. You may address a challenge concerning Spypoint's compliance with this Policy to the designated individual(s) accountable for such compliance.

MANAGEMENT OF PERSONAL INFORMATION

The name or title and the address, of the individual who is accountable for Spypoint's policies and practices and to whom complaints or inquiries can be forwarded are

Legal assistant
info@spypoint.com

DETAILS OF THE POLICY

1. ACCOUNTABILITY

Spypoint is responsible for, and will be able to demonstrate compliance with this Policy, and has designated an individual or individuals accountable for Spypoint's compliance with the Policy.

Accountability for Spypoint's compliance with this Policy rests with the designated individual(s), even though other individuals within Spypoint may be responsible for the day-to-day collection and Processing of Personal Information. Other individuals within Spypoint may be delegated to act on behalf of the designated individual(s).

The identity of the individual(s) designated by Spypoint to oversee Spypoint's compliance with this Policy will be made known upon request if not specified herein.

Any reference to Spypoint in this Policy refers to situations where Spypoint acts as Controller and excludes situations where Spypoint acts as Intermediary, unless specified otherwise.

Where Spypoint determines the purposes and means of Processing jointly with another Controller, Spypoint and such other Controller will be joint Controllers who, in a transparent manner, will determine their respective duties and responsibilities for compliance with the obligations under the applicable laws and regulations, by means of an arrangement between them (the essence of which will be made available to you) reflecting their respective roles and relationships vis-à-vis you. Irrespective of the terms of the arrangement, you may exercise your rights under the applicable laws and regulations in respect of and against each of those joint Controllers.

2. PURPOSES AND PURPOSE LIMITATION

The purposes for which Personal Information is collected will generally be identified by Spypoint at or before the time the Personal Information is collected, for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

Spypoint will document the purposes for which Personal Information is collected. Depending upon the way in which the Personal Information is collected, this can be done orally or in writing. An online application form or notes related thereto, for example, may give notice of the purposes.

Identifying the purposes for which Personal Information is collected at or before the time of collection allows Spypoint to determine the Personal Information it needs to collect to fulfil these purposes. Spypoint will collect only the Personal Information necessary for the purposes that have been identified.

Unless stated otherwise at or before the time the Personal Information is collected the specified, explicit and legitimate purposes for which Spypoint may collect your Personal Information include:

- providing, maintaining, personalizing and improving the services and any of Spypoint's products;
- allowing Spypoint to perform internal operations in relation to its services; and
- sending or facilitating communications between Spypoint and you in relation to the services.

When Personal Information that has been collected is to be used for a purpose not previously identified, the new purpose will be identified and documented prior to Processing and Spypoint will provide you prior to that further Processing with information on that other purpose and with any relevant further information as referred to in section 9 of this Policy [Individual Access and Other Rights], unless you already have the information. Unless the new purpose is required by law, your Consent will be requested before Personal Information can be used for that purpose.

Spypoint will be able to explain to you the purposes for which the Personal Information is being collected.

If the purposes for which Spypoint processes Personal Information do not or do no longer require your identification by Spypoint, Spypoint will not be obliged to maintain, acquire or process additional information in order to identify you for the sole purpose of complying with applicable laws and regulations. However, in such cases, Spypoint will not refuse to take additional information that you provide in order to support the exercise of your rights relating to Processing of your Personal Information.

3. CONSENT

Your knowledge and Consent are required for the Processing of Personal Information, except where inappropriate. (For example, legal, medical, or security reasons may make it impossible or impractical to seek Consent.)

3.1. Consent in General

Your Consent to the Processing of your Personal Information will be unambiguous, manifest, freely given and enlightened, and will be given for specific purposes by a statement or by a clear affirmative action. Such Consent will be valid only for the length of time needed to achieve the purposes for which it was requested.

Spypoint will be able to demonstrate that you have Consented to Processing of your Personal Information where such Processing is based on Consent.

Typically, Spypoint will seek Consent for the Processing of the Personal Information at or before the time of collection. In certain circumstances, Consent with respect to Processing may be sought after the Personal Information has been collected but before use (for example, when Spypoint wants to use Personal Information for a purpose not previously identified).

To make the Consent meaningful, the purposes for which the Personal Information will be used will be stated in such a manner that you can reasonably understand how the Personal Information may be used or disclosed.

Spypoint will not, as a condition of the performance of a contract, including the supply of a product or service, require your Consent to the Processing of Personal Information beyond that required for the performance of that contract or to otherwise fulfil the purposes.

The form of the Consent sought by Spypoint may vary, depending upon the circumstances and the type of Personal Information. In determining the form of Consent to use, Spypoint will take into account the sensitivity of the Personal Information.

The way in which Spypoint seeks Consent may vary, depending on the circumstances and the type of Personal Information collected. Spypoint will generally seek express Consent when the Personal Information is likely to be considered sensitive. Implied Consent may generally be appropriate when the Personal Information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney). Consent will not be obtained through deception.

You can give Consent in many ways. For example:

- an online application form may be used to seek Consent, collect Personal Information and inform you of the use that will be made of the Personal Information. By completing and sending the form, you are giving Consent to the collection and the specified uses;
- a checkbox may be used to allow you to expressly agree that your name and address be given to other organizations;
- Consent may be given orally when Personal Information is collected over the telephone; or
- Consent may be given at the time that you use a product or service.

If your Consent is given in the context of a written declaration which also concerns other matters, the request for Consent will be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

You may withdraw Consent at any time, subject to legal or contractual restrictions and reasonable notice, as easily as it is to give Consent. Such withdrawal will not affect the lawfulness of Processing based on Consent before its withdrawal, and you be informed thereof prior to giving Consent.

Consent to the disclosure of Personal Information from a Third Party may be given by you to Spypoint in order to collect the Personal Information from the Third Party.

Spypoint will collect Personal Information only from you, unless you Consent to collection from Third Partys. However, Spypoint may, without your Consent, collect Personal Information from a Third Party if the law so authorizes. It may also do so if it has a serious and legitimate reason and either of the following conditions is fulfilled:

- the Personal Information is collected in your interest and cannot be collected from you in due time; or

- collection from a Third Party is necessary to ensure the accuracy of the Personal Information.

The Platform is hosted in Canada, and is intended for, amongst others, Canadian, American and European visitors. When we proceed to such transfer of your Personal Information from the European Union to Canada, we use various mechanisms to ensure that your Personal Information is appropriately protected.

3.2. Child's Consent in Relation to Information Society Services

Where a child gives Consent to the Processing of his or her Personal Information for one or more specific purposes in relation to the offer of services normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services, the child must be at least 16 years old unless such Consent for such Processing is given or authorized by the holder of parental responsibility over the child.

Spypoint will make reasonable efforts to verify in such cases that Consent is given or authorized by the holder of parental responsibility over the child, taking into consideration available technology.

4. LIMITED COLLECTION, DATA MINIMIZATION, FAIRNESS AND LAWFULNESS

The collection of Personal Information will be adequate, relevant and limited to that which is necessary for the purposes identified by Spypoint for which it is processed. Information will be collected by fair and lawful means.

Spypoint will specify the type of Personal Information collected as part of its information-handling policies and practices. Personal Information collected may include, but is not limited to your first and last name, your language, your postal and email address, your telephone number and information about your credit card.

If you visit the Platform, you are logged into your account and have a Spypoint connected device, we may record adjustments you make to such device's settings through the Platform interface. We may store such data along with information about your Spypoint device, such as the name and model of such device, its serial number and SIM card number as well as its purchase date, data collected by the device, a history of your device settings and any other information collected about your use of Spypoint's products and services in general.

We could also log information collected through cookies and other tracking technology in order to collect information about your browsing behavior when you visit the Platform, such as your page views, IP address, length of visits on the Platform, etc. We may also collect and log information on your browser type and version. However, such information is collected on an anonymous aggregate basis, which means no Personal Information is associated with this information. Most Internet browsers automatically accept cookies, but you may be able to change the settings of your browser to reject cookies. If you set your browser to reject cookies, parts of the Platform and/or services may however not be

accessible to you.

Spypoint may choose to refrain from requiring your Consent for the Processing of Personal Information relating to you if and to the extent that Processing is necessary:

- (a) for the performance of a contract to which you are a party or in order to take steps at your request prior to entering into a contract;
- (b) for compliance with a legal obligation to which Spypoint is subject;
- (c) in order to protect your vital interests or those of another natural person;
- (d) for the performance of a task carried out in the public interest or in the exercise of official authority vested in Spypoint;
- (e) for the purposes of the legitimate interests pursued by Spypoint or by a third party, except where such interests are overridden by your interests or fundamental rights and freedoms which require protection of Personal Information.

Spypoint may establish a file on you.

Spypoint, when establishing a file on you or recording Personal Information in such a file, will make an entry indicating the source of any Personal Information collected from a Third Party when the Third Party is a person carrying on an enterprise. The entry is part of your file.

Spypoint may not refuse to respond to a request for goods or services or to a request relating to employment by reason of the applicant's refusal to disclose Personal Information except where:

- collection of that Personal Information is necessary for the conclusion or performance of a contract;
- collection of that Personal Information is authorized by law; or
- there are reasonable grounds to believe that the request is not lawful.

Spypoint will not process Personal Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, or genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, unless one of the situations enumerated in GDPR Article 9(2) applies.

The Platform may contain links to third-party websites, which are not under the control of Spypoint. These third-party websites may collect information, such as Personal Information, about you. We invite you to consult the Personal Information management policies applicable to such third-party websites, as they may differ from this Policy.

5. LIMITED USE, DISCLOSURE AND RETENTION

Personal Information will not be processed for purposes other than those for which it was collected, except with your Consent or as required by law.

Personal Information will be retained only as long as necessary for the fulfilment of those purposes in a form which permits your identification for no longer than is necessary for the purposes for which the Personal Information is processed.

Spypoint will develop guidelines and implement procedures with respect to the retention and destruction of Personal Information. These guidelines and procedures will include minimum and maximum retention periods. (Spypoint may be subject to legislative requirements with respect to retention periods.)

Spypoint will not disclose to a Third Party your Personal Information unless you Consent thereto, or such disclosure or use is provided for by law.

For instance, in the carrying on of its enterprise, Spypoint's authorized employees, mandataries or agents or any supplier into a contract with Spypoint for work or services may have access to Personal Information without your Consent if the Personal Information is needed for the performance of their duties or the carrying out of their mandates or contracts.

Spypoint may, without your Consent, disclose Personal Information contained in a file to an archival agency if the archival agency is a person whose object is the acquisition and preservation of documents for their general informational value and if the Personal Information is disclosed as part of the transfer or deposit of the archives of Spypoint.

Personal Information may also be disclosed without your Consent for research purposes if the documents containing the Personal Information are not structured so as to allow retrieval by reference to your name or identifying code or symbol and the Personal Information cannot be retrieved by means of such a reference.

Any person holding Personal Information on behalf of Spypoint may refer to the latter every request for access or rectification received from an individual to whom Personal Information relates.

6. ACCURACY, INTEGRITY, CONFIDENTIALITY AND RIGHT TO RECTIFICATION

Personal Information will be as accurate, complete and kept up-to-date as is necessary for the purposes for which it is to be used. Every reasonable step will be taken to ensure that Personal Information that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.

Personal Information that is used on an ongoing basis, including Personal Information that may be disclosed to third parties, will be generally accurate and up-to-date, unless limits to the requirement for accuracy are set out.

Spypoint will not routinely update Personal Information, unless such a process is necessary to fulfil the purposes for which the Personal Information was collected.

The extent to which Personal Information will be accurate, complete and up-to-date will depend upon input (i) from you or (ii) resulting from data generated by you using Spypoint products or services, and the use of the Personal Information, taking into account your interests.

You will have the right to obtain from Spypoint without undue delay the rectification of inaccurate Personal Information concerning you. Taking into account the purposes of the Processing, you will have the right to have incomplete Personal Information completed, including by means of providing a supplementary statement.

7. SAFEGUARDS

Personal Information will be protected by security safeguards appropriate to the sensitivity of the Personal Information, including protection against unauthorized or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

7.1. Security measures

Spypoint will take the security measures necessary to ensure the protection of the Personal Information processed and that are reasonable given the sensitivity of the Personal Information, the purposes for which it is to be used, the quantity and distribution of the Personal Information and the medium on which it is stored.

The security safeguards of Spypoint will protect Personal Information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification.

The nature of the safeguards will vary depending on the sensitivity of the Personal Information that has been collected, the amount, distribution and format of the Personal Information and the method of storage.

The methods of protection will include:

- physical measures (such as restricted access to offices);
- organizational measures (such as security clearances); and
- technological measures (such as the use of passwords).

Spypoint will make its employees aware of the importance of maintaining the confidentiality of Personal Information, and care will be used in the disposal or destruction of Personal Information, to prevent unauthorized parties from gaining access to the Personal Information.

Spypoint will implement appropriate technical and organizational measures to ensure and to be able to demonstrate that Processing is performed in accordance with applicable laws and regulations, taking into account the nature, scope, context and purposes of Processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons. Those measures will be reviewed and updated where necessary. Where proportionate in relation to Processing activities, such measures will include the implementation of appropriate data protection policies by Spypoint.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Spypoint will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including *inter alia* as appropriate:

- (a) the Pseudonymisation and encryption of Personal Information;
- (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;
- (c) the ability to restore the availability and access to Personal Information in a timely manner in the event of a physical or technical incident;
- (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

In assessing the appropriate level of security, account will be taken in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information transmitted, stored or otherwise processed.

7.2. Data protection by design

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of Processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the Processing, Spypoint will, both at the time of the determination of the means for Processing and at the time of the Processing itself, implement appropriate technical and organizational measures, such as Pseudonymisation, which are designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the Processing in order to meet the requirements of the applicable laws and regulations and protect your rights.

7.3. Data protection by default

Spypoint will implement appropriate technical and organizational measures for ensuring that, by default, only Personal Information which are necessary for each specific purpose of the Processing are processed. That obligation applies to the amount of Personal Information collected, the extent of its Processing, the period of its storage and its accessibility. In particular, such measures will ensure that by default Personal Information is not made accessible without the individual's intervention to an indefinite number of natural persons.

7.4. Intermediaries

Where Processing is to be carried out on behalf of Spypoint, Spypoint will use only Intermediaries providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that Processing will meet the requirements of the applicable laws and regulations and ensure the protection of your rights. The Intermediary will not engage another Intermediary without prior specific or general written authorization of Spypoint. Processing by an Intermediary will be governed by a contract that is binding on the Intermediary with regard to Spypoint and that sets out the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Information and categories of individuals and the obligations and rights of

Spypoint. Where an Intermediary engages another Intermediary for carrying out specific Processing activities on behalf of Spypoint, the same data protection obligations as set out in the contract between Spypoint and the Intermediary will be imposed on that other Intermediary by way of a contract. The Intermediary and any person acting under the authority of Spypoint or of the Intermediary, who has access to Personal Information, will not process those data except on instructions from Spypoint, unless legally required to do so by a statutorily-empowered public authority.

7.5. Notification of a Personal Information Breach

Spypoint will document any Personal Information Breaches, comprising the facts relating to the Personal Information Breach, its effects and the remedial action taken without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the Personal Information Breach to the statutorily-empowered public authority appropriate in accordance with applicable laws and regulations, unless the Personal Information Breach is unlikely to result in a risk to the rights and freedoms of natural persons. Such notification will at least:

- (a) describe the nature of the Personal Information Breach including where possible, the categories and approximate number of individuals concerned and the categories and approximate number of Personal Information records concerned;
- (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- (c) describe the likely consequences of the Personal Information Breach;
- (d) describe the measures taken or proposed to be taken by Spypoint to address the Personal Information Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Spypoint will communicate the Personal Information Breach to you without undue delay when the Personal Information Breach is likely to result in a high risk to the rights and freedoms of natural persons. Such communication will describe in clear and plain language the nature of the Personal Information Breach, and contain at least the information and measures referred to in points (b), (c) and (d) above.

8. OPENNESS AND TRANSPARENCY

Spypoint will make readily available to you specific information about its policies and practices relating to the management of Personal Information.

Spypoint is open about its policies and practices with respect to the management of Personal Information. You will be able to acquire information about Spypoint's policies and practices without unreasonable effort. This information will be made available in a form that is generally understandable.

Spypoint may make information on its policies and practices regarding Personal Information Protection available in a variety of ways. The method chosen depends on the nature of its business and other considerations.

Spypoint will take appropriate measures to provide in a concise, transparent, intelligible and easily accessible form, using clear and plain language, any information that must be provided to you (whether Personal Information is collected from you, or have not been obtained from you subject to situations where the Personal Information must remain confidential due to an obligation of professional secrecy) and any communication regarding your rights relating to Processing of your Personal Information.

More specifically, whether Personal Information is collected from you, or have not been obtained from you, Spypoint will, at the time when Personal Information is obtained (or, where Personal Information have not been obtained from you, within a reasonable period after obtaining the Personal Information, but at the latest within one month, having regard to the specific circumstances in which the Personal Information is processed), provide you with the following information, unless (i) you already have it, or (ii) the provision of such information proves impossible or would involve a disproportionate effort, or (iii) the Personal Information must remain confidential subject to an obligation of professional secrecy:

- (a) Spypoint identity and contact details and, where applicable, of Spypoint's representatives (including the representatives' titles and addresses) accountable for Spypoint's policies and practices and to whom complaints or inquiries can be forwarded;
- (b) the purposes of the Processing for which the Personal Information is intended as well as the legal basis for the Processing;
- (c) the legitimate interests pursued by the Spypoint or by a third party here where the Processing is necessary for purposes of the legitimate interests pursued by Spypoint or by a third party;
- (d) a description of the type of Personal Information held by Spypoint, including a general account of its use, and the categories of Personal Information concerned;
- (e) the Recipients or categories of Recipients of the Personal Information, if any, including what Personal Information is made available to related organizations (e.g. affiliates such as subsidiaries and parent organizations);
- (f) the means of gaining access to Personal Information held by Spypoint; and
- (g) where applicable, the fact that Spypoint intends to transfer Personal Information to a third country or international organization and the existence or absence of an adequacy decision within the meaning of the GDPR, or reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

Spypoint will, at the time when Personal Information is obtained, provide you with the following further information necessary to ensure fair and transparent

Processing, unless you already have it:

- (a) the period for which the Personal Information will be stored, or if that is not possible, the criteria used to determine that period;
- (b) the existence of the right to request from Spypoint access to and rectification or erasure of Personal Information or Restriction of Processing concerning you or to object to Processing as well as the right to data portability;
- (c) where the Processing is based on your Consent, the existence of the right to withdraw Consent at any time, without affecting the lawfulness of Processing based on Consent before its withdrawal;
- (d) the right to lodge a complaint with a statutorily-empowered public authority;
- (e) from which source the Personal Information originates (if it does not originate from you), and if applicable, whether it came from publicly accessible sources;
- (f) whether the provision of Personal Information is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether you are obliged to provide the Personal Information and of the possible consequences of failure to provide such data; and
- (g) the existence of automated decision-making, including Profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for you.

The above-listed elements may be provided in combination with standardized icons (which may be machine-readable) in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended Processing.

9. INDIVIDUAL ACCESS AND OTHER RIGHTS

Upon request, you will be informed of the existence and Processing of your Personal Information and will generally be given access to that Personal Information. You will be able to challenge the accuracy and completeness of the Personal Information and have it amended as appropriate.

9.1. Right of Access

Upon request, Spypoint will inform you whether or not Spypoint holds Personal Information about you and may indicate the source of this Personal Information. Spypoint will generally allow you access to this Personal Information. You may be required to provide sufficient information to permit Spypoint to provide an account of the existence and Processing of Personal Information.

You are entitled to obtain that any Personal Information collected otherwise than lawfully be deleted.

No request for access, rectification or deletion may be considered unless it is

made in writing by you when you prove that you are the individual concerned (or the representative, heir or successor of that individual, or the liquidator of the succession, a beneficiary of life insurance or of a death benefit).

Spypoint, when holding a file that is the subject of your request for access, rectification or deletion, will respond to that request within a reasonable time after receipt of the request, without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. Spypoint will inform you of any such extension within one month of receipt of the request, together with the reasons for the delay. The requested information will be provided or made available in a form that is generally understandable. (For example, if Spypoint uses abbreviations or codes to record Personal Information, an explanation will be provided.)

The information will be provided in writing, or by other means, including, where appropriate, by electronic means. Where you make the request by electronic form means, the information will be provided by electronic means in a commonly used electronic form where possible, unless otherwise requested by you. When requested by you, the information may be provided orally, provided that your identity is proven by other means.

Spypoint will facilitate the exercise of your rights relating to Processing of your Personal Information and will not refuse to act on your request for exercising such rights unless Spypoint is not in a position to identify you.

In certain situations, Spypoint may not be able to provide access to all the Personal Information it holds about you. Exceptions to the access requirement are meant to be limited and specific. The reasons for denying access will be provided to you upon request.

Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security or commercial proprietary reasons and information that is subject to solicitor-client or litigation privilege.

Spypoint may refuse to give communication of Personal Information to you where disclosure of the Personal Information would be likely to hinder an inquiry the purpose of which is the prevention, detection or repression of crime or statutory offences.

Spypoint will refuse to give communication of Personal Information to you where (i) disclosure would be likely to reveal Personal Information about a Third Party or the existence of Personal Information and (ii) the disclosure may seriously harm that Third Party, unless the latter consents to the disclosure of the Personal Information or in the case of an emergency that threatens the life, health or safety of an individual.

If Spypoint does not take action on your request, Spypoint will inform you without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a statutorily-empowered public authority and seeking a judicial remedy.

The transcription, reproduction or transmission of Personal Information and any communication and actions taken in relation to such transcription, reproduction or

transmission will be provided free of charge, unless your requests are manifestly unfounded or excessive, in particular because of their repetitive character, in which case Spypoint may either refuse to act on the request or charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested. For any further copies requested by you, Spypoint may charge a reasonable fee based on administrative costs.

9.2. Right to Erasure ('Right to be Forgotten')

You will have the right to obtain from Spypoint the erasure of Personal Information concerning you without undue delay and Spypoint will have the obligation to erase Personal Information without undue delay where one of the following grounds applies:

- (a) the Personal Information is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
- (b) you withdraw Consent on which the Processing is based, and where there is no other legal ground for the Processing;
- (c) you object to the Processing and there are no overriding legitimate grounds for the Processing;
- (d) the Personal Information has been unlawfully processed;
- (e) the Personal Information has to be erased for compliance with a legal obligation to which Spypoint is subject;
- (f) the Personal Information has been collected in relation to the offer of services normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

Where Spypoint has made Personal Information public and is obliged to erase such Personal Information, Spypoint, taking account of available technology and the cost of implementation, will take reasonable steps, including technical measures, to inform Controllers who are Processing the Personal Information that you have requested the erasure by such Controllers of any links to, or copy or replication of, those Personal Information.

Such right to erasure will not apply to the extent that Processing is necessary:

- (a) for exercising the right of freedom of expression and information;
- (b) for compliance with a legal obligation which requires Processing by a statutorily-empowered public authority to which Spypoint is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in Spypoint;
- (c) for reasons of public interest in the area of public health;

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right to erasure is likely to render impossible or seriously impair the achievement of the objectives of that Processing; or

(e) for the establishment, exercise or defence of legal claims.

9.3. Right to Restriction of Processing

You will have the right to obtain from Spypoint Restriction of Processing where one of the following applies:

(a) the accuracy of the Personal Information is contested by you, for a period enabling Spypoint to verify the accuracy of the Personal Information;

(b) the Processing is unlawful and you oppose the erasure of the Personal Information and requests the restriction of their use instead;

(c) Spypoint no longer needs the Personal Information for the purposes of the Processing, but they are required by you for the establishment, exercise or defence of legal claims;

(d) you have objected to Processing pending the verification whether the legitimate grounds of Spypoint override yours.

Where Processing has been restricted pursuant to the foregoing, such Personal Information will, with the exception of storage, only be processed with your Consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of a statutorily-empowered public authority.

If you have obtained Restriction of Processing pursuant to the foregoing, you will be informed by Spypoint before the Restriction of Processing is lifted.

9.4. Right to Data Portability

You will have the right to receive the Personal Information which you have provided to Spypoint, in a structured, commonly used and machine-readable format and have the right to transmit those data to another Controller without hindrance from Spypoint to which the Personal Information has been provided, where the Processing is based on Consent and the Processing is carried out by automated means.

9.5. Right to Object

You will have the right to object, on grounds relating to your particular situation, at any time to Processing of Personal Information concerning you which is necessary for the purposes of the legitimate interests pursued by Spypoint or by a third party or for the performance of a task carried out in the public interest or in the exercise of official authority vested in Spypoint, including Profiling based on those provisions. Spypoint will no longer process the Personal Information unless

Spypoint demonstrates compelling legitimate grounds for the Processing which override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

9.6. Automated Individual Decision-Making, Including Profiling

If, when or where applicable, you will have the right not to be subject to a decision based solely on automated Processing, including Profiling, which produces legal effects concerning yourself or similarly significantly affects you, but will not apply if the decision:

- (a) is necessary for entering into, or performance of, a contract between you and Spypoint;
- (b) is authorized by the law to which Spypoint is subject and which also lays down suitable measures to safeguard your rights and freedoms and legitimate interests; or
- (c) is based on your explicit Consent.

In the cases referred to in points (a) and (c) above, Spypoint will implement suitable measures to safeguard the right to obtain human intervention on the part of Spypoint, to express your point of view and to contest the decision.

10. CHALLENGING COMPLIANCE

You may address a challenge concerning Spypoint's compliance with this Policy to the designated individual(s) accountable for such compliance.

Spypoint has put procedures in place to receive and respond to complaints or inquiries about its policies and practices relating to the handling of Personal Information. The complaint procedure is meant to be easily accessible and simple to use.

Spypoint will inform individuals who make inquiries or lodge complaints of the existence of the relevant complaint procedure.

Spypoint will investigate all complaints. If a complaint is found to be justified, Spypoint will take appropriate measures, including, if necessary, amending its policies and practices.

When a challenge is not resolved to your satisfaction, the substance of the unresolved challenge will be recorded by Spypoint.