RegiÔtels

You look after the guest,
we look after the rest

GDPR COMPLIANCE MANUAL

RegiOtels International SARLs
2 rue de la Chapelle, L-1325, Luxembourg, B-232714, VAT No. LU31032975
info@regiotels.com : +352 621 136 765

INDEX

Personal Data Protection Policy

The Board of Directors of Regiotels International, S.à.r.l (the **"Company"**) has the power to design, assess and continuously revise the Governance and Sustainability System, and specifically to approve and update the corporate policies, which contain the guidelines governing the conduct of the Company and of the companies belonging to the group of which the Company is the controlling entity, within the meaning established by law (the **"Group"**).

In fulfilling these responsibilities, and within the framework of the law and the *By-Laws*, the guidelines for conduct that take shape in the *Purpose and Values of the RegiOtels group*, and its sustainable development strategy, the Board of Directors hereby approves this *Personal Data Protection Policy* (the ***"Policy"***).

1. Purpose

The purpose of this *Policy* is to establish the common and general principles and guidelines for conduct that are to govern the Group as regards personal data protection, ensuring compliance with applicable law under all circumstances.

In particular, this *Policy* guarantees the right to the protection of personal data for all natural persons who establish relations with the companies belonging to the Group, ensuring respect for the rights to reputation and to privacy in the processing of the various categories of personal data from different sources and for various purposes based on their business activities, all in compliance with the Company's *Policy on Respect for Human Rights*.

2. Scope of Application

This *Policy* applies to all companies of the Group, as well as to all investees not belonging to the Group over which the Company has effective control, within the limits

established by law, and to all people engaging in relations with entities belonging to the Group.

Without prejudice to the provisions of the preceding paragraph, listed country sub-holding companies and their subsidiaries, based on their own special framework of strengthened autonomy, may establish an equivalent policy, which must be in accord with the principles set forth in this *Policy* and in the other environmental, social and corporate governance and regulatory compliance policies of the Governance and Sustainability System.

At those companies in which the Company has an interest and to which this *Policy* does not apply, the Company will promote, through its representatives on the boards of directors of such companies, the alignment of their own policies with those of the Company.

This *Policy* shall also apply, to the extent relevant, to the joint ventures, temporary joint ventures and other equivalent associations, if the Company assumes the management thereof.

3. General Principles relating to the Processing of Personal Data

Group companies shall thoroughly comply with personal data protection law in their jurisdiction, the laws that apply based on the processing of personal data that they carry out and the laws determined by binding rules or resolutions adopted within the Group.

Group companies shall also strive to ensure that the principles set forth in this *Policy* are taken into account (i) in the design and implementation of all procedures involving the processing of personal data; (ii) in the products and services offered thereby; (iii) in all contracts and obligations that they formalize with natural persons; and (iv) in the implementation of any systems and platforms that allow access by Group professionals or third parties to personal data and the collection or processing of such data.

4. Main Principles relating to the Processing of Personal Data

The principles relating to the processing of personal data on which this *Policy* is based are described below:

a) Principle of legitimate, lawful and fair processing of personal data.

The processing of personal data shall be legitimate, lawful and fair, in accordance with applicable law. In this sense, personal data must be collected for one or more specific and legitimate purposes in accordance with applicable law.

When so required by law, the consent of the data subjects must be obtained before their data are collected.

Also when so required by law, the purposes for processing the personal data shall be explicit and specific at the time of collection thereof.

In particular, Group companies shall not collect or process personal data relating to ethnic or racial origin, political ideology, beliefs, religious or philosophical convictions, sexual orientation or practices, trade union membership, data concerning health, or genetic or biometric data for the purpose of uniquely identifying a person, unless the collection of said data is necessary, legitimate and required or permitted by applicable law, in which case they shall be collected and processed in accordance with the provisions thereof.

b) Principle of minimisation.

Only personal data that are strictly necessary for the purposes for which they are collected or processed and adequate for such purposes shall be processed.

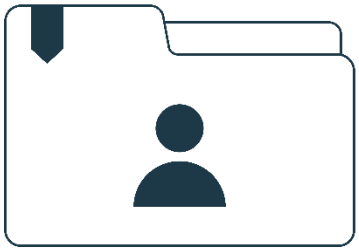
c) Principle of accuracy.

Personal data must be accurate and up-to-date. They must otherwise be erased or rectified.

d) Principle of storage duration limitation.

Personal data shall not be stored for longer than is necessary for the purposes for which they are processed, except in the circumstances established by law.

e) Principles of integrity and confidentiality.



Personal data must be processed in a manner that uses technical or organisational measures to ensure appropriate security that protects the data against unauthorised or unlawful processing and against loss, destruction or accidental damage.

The personal data collected and processed by Group companies must be stored with the utmost confidentiality and secrecy, may not be used for purposes other than those that justified and permitted the collection thereof, and may not be disclosed or transferred to third parties other than in the cases permitted by applicable law.

f) Principle of proactive responsibility (accountability).

Group companies shall be responsible for complying with the principles set forth in this *Policy* and those required by applicable law and must be able to demonstrate compliance when so required by applicable law.

Group companies must perform a risk assessment of the processing that they carry out in order to identify the measures to apply to ensure that personal data are processed in accordance with legal requirements. When so required by law, they shall perform a prior assessment of the risks that new products, services or IT systems may involve for personal data protection and shall adopt the necessary measures to eliminate or mitigate them.

Group companies must maintain a record of activities in which they describe the personal data processing that they carry out in the course of their activities.

In the event of an incident causing the accidental or unlawful destruction, loss or alteration of personal data, or the disclosure of or unauthorised access to such data, the internal protocols established for such purpose by the Company's Corporate Security Division or by such division as may assume the duties thereof and those that are established by applicable law must be followed. Such incidents must be documented and measures shall be adopted to resolve and mitigate potential adverse effects for data subjects.

In the cases provided for by law, data protection officers shall be designated in order to ensure that Group companies comply with the legal provisions on data protection.

g) Principles of transparency and information.

Personal data shall be processed in a transparent manner in relation to data subjects, with the provision to data subjects of intelligible and accessible information regarding the processing of their data when so required by applicable law.

For purposes of ensuring fair and transparent processing, the Group company that is responsible for the processing must inform data subjects whose data are to be collected of the circumstances relating to the processing in accordance with applicable law.

h) Acquisition or procurement of personal data.

It is forbidden to purchase or obtain personal data from unlawful sources, from sources that do not sufficiently ensure the lawful origin of such data or from sources whose data have been collected or transferred in violation of the law.

i) Engagement of data processors.

Prior to engaging any service provider that may have access to personal data for which Group companies are responsible, as well as during the effective term of the contractual relationship, such Group companies must adopt the necessary measures to ensure and, when legally required, demonstrate, that the data processing by the data processor is performed in accordance with applicable law.

j) International transfers of data.

Any processing of personal data that is subject to European Union regulations and entails a transfer of data outside the European Economic Area must be carried out strictly in compliance with the requirements established by applicable law in the jurisdiction of origin. In addition, Group companies located outside the European Union must comply with any requirements for international transfers of personal data that are applicable in their respective jurisdictions.

k) Rights of data subjects.

Group companies must allow data subjects to exercise the rights of access, rectification, erasure, restriction of processing, portability and objection that are applicable in each jurisdiction, establishing for such purpose such internal procedures as may be necessary to at least satisfy the legal requirements applicable in each case.

5. Implementation

Pursuant to the provisions of this *Policy*, the Corporate Security Division, together with the Company's Legal Services or such divisions as may assume the duties thereof, shall develop and keep updated internal rules for global data protection management at the Group level, which shall be implemented by said division and which shall be mandatory for all members of the management team and professionals of the Company.

Likewise, the Corporate Security Division and the Legal Services Division of each country, or such divisions as may assume the duties thereof, shall establish local internal procedures designed to implement the principles laid down in this *Policy* and to adapt the content thereof in accordance with applicable law in their respective jurisdictions.

The Legal Services Division of each country, or such division as may assume the duties thereof, shall be responsible for informing the Company's Corporate Security Division of regulatory developments and news that occur in the area of personal data protection.

The Company's Systems Division, or such division as may assume the duties thereof, shall be responsible for implementing the information technology systems of the companies of the Group, the information technology controls and developments that are appropriate to ensure compliance with the internal rules for global data protection management, and shall ensure that said developments are updated at all times.

In addition, the businesses and corporate divisions must (i) subject to the provisions of applicable law in each case, appoint the persons responsible for the data, who shall act on a coordinated basis and under the supervision of the Company's Corporate Security Division; and (ii) coordinate with the Corporate Security Division any activity that involves or entails the management of personal data, in all cases adhering to the special framework of strengthened autonomy of the listed country subholding companies.

Finally, the Cybersecurity Committee, created pursuant to the provisions of the *Cybersecurity Risk Policy*, shall monitor the general status of personal data protection at companies of the Group and shall endeavour to ensure proper Group-level coordination of risk practices and management in the area of personal data protection, assisting the Corporate Security Division in the approval of rules in the area of cybersecurity and data protection.

6. Control and Evaluation

a) Control

The Corporate Security Division, or the division assuming the duties thereof, shall supervise compliance with the provisions of this *Policy* by the Company and the other entities of the Group. The foregoing shall in any event be without prejudice to the responsibilities vested in other bodies and divisions of the Company and, if applicable, in the management decision-making bodies of the companies within the Group.

Regular audits shall be performed with internal or external auditors in order to verify compliance with this *Policy*.

b) Evaluation

The Corporate Security Division, or any division assuming the duties thereof, shall evaluate compliance with and the effectiveness of this *Policy* at least once per year and shall report to the Finance, Control and Corporate Development Division, or to the division assuming such duties at any particular time, on the results of such evaluation.

This *Policy* was initially approved by the Board of Directors on 15 December 2021 and was last amended on 4 February 2022.

Privacy Notice

RegiÔtels aims to be fully GDPR compliant. We collect cookie information about our visitors for a few reasons: statistical purposes to track how many users we have and how often you visit our website collection of information to monitor behavior on the site and improve our services. We do not monitor individual traffic patterns on our site and we will do our utmost to respect your privacy.

Collecting of information

We do collect information on our users through Google Analytics, and when you sign up for our newsletter. If you have signed up for our newsletter in the past or future, or given us your email address because of something else, we will not sell or pass on your details to any other company.

How do we protect your information?

Your personal information is contained behind secured networks and is only accessible by a limited number of persons who have special access rights to such systems, and are required to keep the information confidential. In addition, all information you supply is encrypted via Secure Socket Layer (SSL) technology. We implement a variety of security measures when a user enters, submits, or accesses their information to maintain the safety of your personal information. However, no online data transmission can be guaranteed to be 100% secure.

What is a cookie?

A cookie is a small text file with data stored by your browser on your computer. If you visit the website another time, a cookie will make sure that your browser is recognized. For example, your settings for log-ins can be preserved, or the website shows information that may be of interest to you more clearly. Cookies can also be used for statistical purposes. Cookies are always anonymous and your personal information will not be known until you leave it.

Third Parties

Third party advertisers such as Google Analytics, Google Adwords or Sendinblue will generate statistical cookies to track advertising impressions and conversions. The use of cookies by third parties is subject to those companies' own privacy and cookie policies. For more on Google's privacy policy, follow the link. Here is also a Chrome extension which Google developed to be able to opt out of their Analytics program: tools.google.com/dlpage/gaoptout?hl=en
By using the regiotels.com website you are agreeing to the use of cookies as described. Some advertisers may tailor advertising to specific groups of advertisers using cookies.

Readers can opt out from online behavioral advertising using the following methods: Use the Online Choices opt-out tool provided at www.youronlinechoices.com/opt-out. Change your computer's browser settings to block, delete, and/or control the use of all third-party cookies. Refer to your computer's web browser's documentation for more information.

Why do we ask for Passwords?

In order to properly work with you, RegiÔtels will have to have access to certain accounts, such as (but not limited to): booking.com, your website, expedia.com, your domain and hosting provider, other OTAs (Online Travel Agencies), Google My Business, or Google Analytics.

This is done so that we can get a full picture of your hotel and its online representation. It also allows us to improve your online presence and to make the necessary changes for you to increase your revenue, your visibility, and to ascertain what we can do to properly help you.

Your passwords and all your sensitive data will never be given to any third parties. Only some of the core team of RegiÔtels will have access to this information which is necessary for them to make suggestions and improvements. All employees have to sign an NDA (non-disclosure agreement) which prevents them from propagating your

passwords and your sensitive data to anyone else. If you'd like to know exactly who has access to what, please feel free to get in touch with us on digital@regiotels.com.

Social Media

On the RegiÔtels website, you can share information via social media, via the available social media buttons (such as on the blog page). The relevant social media can place cookies via these buttons. We have no influence on the use of these cookies by these parties. They are responsible for the use and provision of data obtained in this way. The privacy policy and the general terms and conditions of the social media platforms involved apply to this use. Find the privacy policies of the relevant social media platforms below:
Facebook | YouTube | LinkedIn | Instagram | Xing

Recruiting Statement

By sending us your CV or other personal information in response to a vacancy or as part of a spontaneous application, you confirm that we may use and transfer data as described in this privacy policy.

You may provide personal information to us related to education, employment, contacts, preferences, job qualifications, and jobs when you submit an application. We recommend that you do not disclose sensitive personal information (e.g., height, weight, religion, philosophical or political beliefs, financial data, sexual orientation, membership of a trade union or political party) in your CV or any materials in support of your application. To the extent you provide sensitive personal information, you expressly authorize Stardekk to handle such details as specified in this Statement.

We will use your personal information for recruitment purposes and if you are offered a job or are employed by RegiÔtels, we will use it for other employment-related purposes.

We may also retain your information after the recruitment process is completed in order to contact you about potential future opportunities for a period of three years from the date of your application. However, it is possible that we may keep your data in anonymous form for longer for statistical purposes

Questions

If you have questions about the privacy statement or the use of your information, you can get in touch with our Digital Manager via christian@regiotels.com

Employee Privacy Notice

This Employee Privacy Policy ("Privacy Policy") explains what types of personal information we may collect about our employees and how it may be used.

While this Privacy Policy is intended to describe the broadest range of our information processing activities globally, those processing activities may be more limited in some jurisdictions based on the restrictions of their laws. For example, the laws of a country may limit the types of personal information we can collect or the manner in which we process that information. In those instances, we adjust our internal policies and practices to reflect the requirements of local law.

For personal data collected under this Privacy Policy, the controller will be RegiOtels and the RegiOtels affiliates by which you are employed. For, (i) specific security concerns around your data, (ii) in the event you feel that you have not received proper attention to your data request, or (iii) have any other data privacy concerns, please contact hr@regiotels.com.

RegiOtels International, Sàrl. is a global company with its headquarters in Luxembourg. This means that personal information may be used, processed, and transferred throughout the European Union and other countries or territories and those countries or territories may not offer the same level of data protection as the country where you reside, including the European Economic Area. However, RegiÔtels will ensure that appropriate or suitable safeguards are in place to protect your personal information and that transfer of your personal information complies with applicable data protection laws. Where required by applicable data protection laws, RegiOtels has ensured that service providers (including other RegiOtels affiliates) sign standard contractual clauses as approved by the European Commission or other supervisory authority with jurisdiction over the relevant RegiOtels data exporter (which typically will be your employer).

Who is collecting your personal data (who is the data controller)?

The RegiÔtels entity that is a party to your employment contract or contract for services or otherwise employs you will be the data controller of your personal data. The following are the RegiÔtels entities that act as controller: RegiOtels Sàrl, RegiOtels International Sàrl, RegiOtels GmbH, RegiOtels Egypt Co. Ltd, RegiOtels Cambodia Co. Ltd., RegiOtels Thailand Co. Ltd and other RegiÔtels subsidiaries throughout the globe (collectively "RegiÔtels").

RegiÔtels affiliates may act as processors on behalf of other RegiÔtels affiliates and/ or controllers. Furthermore, RegiÔtels, its affiliates and subsidiaries participate in a group-wide IT system in order to harmonize RegiÔtels' IT infrastructure and its use (the "System"). The System also may hold data on all employees, workers, individual contractors and contingent workers ("Staff"). Insofar the System serves to improve and harmonize most of the human resources ("HR") processes within RegiÔtels. RegiOtels International in the Luxembourg is responsible for the System.

Applicability of Other RegiÔtels Privacy Policies

The websites of RegiÔtels (e.g., https://www.regiotels.com/the-story-so-far/) have separate privacy policies and terms of use that apply to their use. Additionally, some of our third party products and services may have separate privacy policies and terms of use that apply to their use. Any personal information collected in connection with your use of those websites or products and services are not subject to this Privacy Policy. If you are unsure how or if this Privacy Policy applies to you, please contact hr@regiotels.com.

Third Party Services

In some cases, you may provide personal information to third parties that RegiÔtels works with or that provide services to RegiÔtels. This includes, those parties identified in the RegiÔtels Tech Partners ("Third Parties").

The RegiÔtels Tech Partners page is updated periodically to ensure accurate, up-to-date disclosure of employee and customer third party applications used at RegiÔtels. This particular policy applies to those applications identified as relating to Employee applications. The use of such Third Party websites may be governed by separate terms of use and privacy policies which are not under our control and are not subject to this Privacy Policy. Please contact such Third Parties for questions regarding their privacy practices, as well as if you would like to have them modify, update, alter or delete your personal information. Please understand that there are exceptions to rights surrounding personal data relating to employment. RegiÔtels is required to maintain certain employment information by law.

What is Personal Information?

Personal information, also known as personally identifiable information or personal data, for purposes of this Privacy Policy means any information that (i) directly and clearly identifies an individual, or (ii) can be used in combination with other information to

identify an individual. Personal information does not include such information if it is anonymous or if it has been rendered de-identified by removing personal identifiers.

Examples of personal information include:

- An individual's name
- Employee or Social Security ID number
- Home address
- Home phone number
- Personal email address
- Names of family members
- Date of birth

What is Sensitive Personal Information?

Sensitive personal information is a subset of personal information that may be more sensitive in nature for the individual concerned.

Examples of sensitive personal information include:

- Race and ethnic information
- Sexual orientation
- Political/religious beliefs
- Social security or other taxpayer/government issued identification numbers
- Financial information
- National identification number or passport information
- Health or medical information, including genetic information
- Criminal records
- And in some regions, such as the European Union, trade union membership

What Personal Information Do We Collect?

We collect and maintain different types of personal information about you in accordance with applicable law. This includes the following:

- Name
- Gender
- Home address
- Telephone number
- Date of birth
- Marital status
- Employee identification number
- Emergency contacts
- Residency
- Work permit status
- Military status
- Nationality
- Passport information
- Social security or other taxpayer/government identification number
- Payroll information, banking details
- Wage and benefit information
- Retirement account information
- Sick pay, Paid Time Off, retirement accounts, pensions, insurance and other benefits information (including the gender, age, nationality and passport information for any spouse, minor children or other eligible dependents and beneficiaries).
- Information from interviews and phone-screenings you may have had, if any.
- Date of hire, date(s) of promotion(s), work history, technical skills, educational background, professional certifications and registrations, language capabilities, and training records.

- Beneficiary and emergency contact information.
- Forms and information relating to the application for, or in respect of changes to, employee health and welfare benefits; including, short and long-term disability, medical and dental care, etc.
- Physical limitations and special needs in order to provide accommodations where possible.
- Records of work absences, vacation/paid time off, entitlement and requests, salary history and expectations, performance appraisals, letters of appreciation and commendation, and disciplinary and grievance procedures (including monitoring compliance with and enforcing our policies).

Where permitted by law and applicable we may collect the results of credit and criminal background checks, screening, health certifications, driving license number, vehicle registration, and driving history.

- Information required for us to comply with laws, the requests and directions of law enforcement authorities or court orders (e.g., child support and debt payment information).
- Acknowledgements regarding our policies, including employee handbooks, ethics and/or conflicts of interest policies, and computer and other corporate resource usage policies.
- Voicemails, e-mails, correspondence, documents, and other work product and communications created, stored or transmitted for professional or job related purposes using our networks, applications, devices, computers, or communications equipment.
- Date of resignation or termination, reason for resignation or termination, information relating to administering termination of employment (e.g. references).
- Letters of offer and acceptance of employment.
- Your resume or CV, cover letter, previous and/or relevant work experience or other experience, education, transcripts, or other information you provide to us in support of an application and/or the application and recruitment process.
- References and interview notes.

- Information relating to any previous applications you may have made to RegiÔtels and/or any previous employment history with RegiÔtels.

For specifics about what information is collected by third party applications, please refer to the RegiÔtels Tech Partner page.

Apart from personal information relating to yourself, you may also provide us with personal data of related parties, notably your dependents and other family members, for purposes of your HR administration and management, including the administration of benefits and to contact your next-of-kin in an emergency. Before you provide such third-party personal data to us you must first inform these third parties of any such data which you intend to provide and of the processing to be carried out by us. You must ensure and secure evidence that these related parties, or their legal representatives if they are minors, have given their free and express consent that their personal data may be processed by RegiÔtels and/or its affiliates and subcontractors for the purposes described in this Privacy Policy.

How is Data Collected?

Generally, we collect personal information directly from you in circumstances where you provide personal information (during the onboarding process, for example). However, in some instances, the personal information we collect has been inferred about you based on other information you provide us, through your interactions with us, or from third parties. When we collect your personal information from third parties it is either because you have given us express consent to do so, your consent was implied by your actions (e.g., your use of a Third-Party employee service made available to you by us), or because you provided explicit consent to the Third-Party to provide the personal information to us. Where permitted or required by applicable law or regulatory requirements, we may collect personal information about you without your knowledge or consent.

We reserve the right to monitor the use of our equipment, devices, computers, network, applications, software, and similar assets and resources for the safety and protection of employees and intellectual property. In the event such monitoring occurs, it may result in the collection of personal information about you. If required by applicable law, we will notify you of such monitoring and obtain your consent.

How We Process and Use Your Personal Information

We may collect and process your personal information in the Systems for various purposes subject to local laws and any applicable collective bargaining agreements and works council agreements, including:

- Recruitment, training, development, promotion, career, and succession planning
- Appropriate vetting for recruitment and team allocation including, where relevant and appropriate, credit checks, right to work verification, identity fraud checks, relevant employment history, relevant regulatory status and professional qualifications
- Providing and administering remuneration, salary, benefits, and incentive schemes and providing relevant information to payroll
- Allocating and managing duties and responsibilities and the business activities to which they relate
- Identifying and communicating effectively with other employees and management
- Managing and operating conduct, performance, capability, absence, and grievance related reviews, allegations, complaints, investigations, and processes and other informal and formal HR processes and making related management decisions
- Consultations or negotiations with representatives of the workforce
- Conducting surveys for benchmarking and identifying improved ways of working employee relations and engagement at work (these will often be anonymous but may include profiling data such as age to support analysis of results)
- Processing information about absence or medical information regarding physical or mental health or condition in order to assess eligibility for incapacity or permanent disability related remuneration or benefits, determine fitness for work, facilitate a return to work, make adjustments or accommodations where possible to duties or the workplace and make management decisions regarding employment or engagement or continued

employment or engagement or redeployment and conduct related management processes

- For planning, managing and carrying out restructuring or redundancies or other change programs including appropriate consultation, selection, alternative employment searches and related management decisions
- Operating email, IT, Internet, intranet, social media, HR related and other company policies and procedures. The company carries out monitoring of RegiÔtels' IT systems to protect and maintain the systems, to ensure compliance with RegiÔtels policies and to locate information through searches where needed for a legitimate business purpose
- Complying with applicable laws and regulation (for example maternity or parental leave legislation, working time and health and safety legislation, taxation rules, worker consultation requirements, other employment laws and regulation to which RegiÔtels is subject in the conduct of its business)
- Monitoring programs to ensure equality of opportunity and diversity with regard to personal characteristics protected under local anti-discrimination laws
- Planning, due diligence and implementation in relation to a commercial transaction or service transfer involving RegiÔtels that impacts on your relationship with RegiÔtels (for example mergers and acquisitions or a transfer of your employment under automatic transfer rules)
- For business operational and reporting documentation such as the preparation of annual reports or tenders for work or client team records including the use of your personal photo
- In order to operate the relationship with Third-Party customer and suppliers including the disclosure of relevant vetting information in line with the appropriate requirements of regulated customers to those customers, contact or professional CV details or resume, or your personal photo for identification to clients or disclosure of information to data processors for the provision of services to RegiÔtels
- Where relevant for publishing appropriate internal or external communications or publicity material including via social media in appropriate circumstances, provided that privacy rights are preserved

- To support HR administration and management and maintaining and processing general records necessary to manage the employment or worker relationship and operate the contract of employment or engagement
- To centralize HR administration and management processing operations in an efficient manner for the benefit of our employees and to change access permissions
- To provide support and maintenance for the System
- To enforce our legal rights and obligations, and for any purposes in connection with any legal claims made by, against or otherwise involving you
- To comply with lawful requests by public authorities (including without limitation to meet national security or law enforcement requirements), discovery requests, or where otherwise required or permitted by applicable laws, court orders, government regulations, or regulatory authorities (including without limitation data protection, tax and employment), whether within or outside your country
- Other purposes permitted by applicable privacy and data protection legislation including where applicable, legitimate interests pursued by RegiÔtels where this is not overridden by the interests or fundamental rights and freedoms of employees.

Legal Basis for processing

Where applicable data protection laws require us to process your personal data on the basis of a specific lawful justification, we generally process your personal data under one of the following bases:

Compliance with a legal obligation to which RegiÔtels is subject; Performance under an employment contract with RegiÔtels; For RegiÔtels' leagitimate interests being those purposes described in the section above headed "How We Process and Use Your Personal Information"; Your consent where required and a legitimate legal basis under applicable local laws.

We may on occasion process your personal data for the purpose of the legitimate interests of a Third-Party where this is not overridden by your interests.

Processing of Special Categories of Personal Data

"Special Categories of Personal Data" includes information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, as well as genetic and biometric data.

From time to time you may provide us with information which constitutes Special Categories of Personal Data or information from which Special Categories of Personal Data may be deduced. In such cases, where required by law, we will obtain your express written consent to our processing of Special Categories of Personal Data. If separate consent is not required by local law, by providing this information to RegiÔtels, you give your freely given, informed, explicit consent for us to process those Special Categories of Personal Data for the purposes set out in How We Process and Use Your Personal Information section above.

You may withdraw your consent at any time by contacting hr@regiotels.com. Where you have withdrawn consent but RegiÔtels retains the personal data we will only continue to process that Special Category Personal Data where necessary for those purposes where we have another appropriate legal basis such as processing necessary to comply with legal obligations related to employment or social security. However, this may mean that we cannot (for example) administer certain benefits or contact your next-of-kin in an emergency or provide support to you above and beyond our legal obligations. You give your knowledgeable, freely given, express consent to RegiÔtels for RegiÔtels to use, disclose and otherwise process any personal health information about you that is provided to RegiÔtels by any of your personal health information custodians, for the purposes set out in the How We Process and Use Your Personal Information section above.

Sharing Personal Information

Your personal information may be shared, including to our affiliates, subsidiaries, and other third parties, as follows:

- Where you request us or provide your consent to us.
- In order to carry out the uses of personal information described above (see, How We Process and Use Your Personal Information). When using or collaborating with third parties in the operation of our business, including in connection with providing many of the benefits and services we offer our employees (e.g., human resources information systems, financial investment service providers, insurance providers). When we share personal information with third parties we typically require that they only use or disclose such

personal information in a manner consistent with the use and disclosure provisions of this Privacy Policy and applicable law.

- We may buy or sell businesses and other assets. In such transactions, employee information is generally one of the transferred business assets and we reserve the right to include your personal information as an asset in any such transfer. Also, in the event that we, or substantially all of our assets, are acquired, your personal information may be one of the transferred assets.
- Where required by law, by order or requirement of a court, administrative agency, or government tribunal, which includes in response to a lawful request by public authorities, including to meet national security or law enforcement requirements or in response to legal process.
- If we determine it is necessary or desirable to comply with the law or to protect or defend our rights or property.
- As necessary to protect the rights, privacy, safety, or property of an identifiable person or group or to detect, prevent or otherwise address fraud, security or technical issues, or to protect against harm to the rights, property or safety of RegiÔtels, our users, applicants, candidates, employees or the public or as otherwise required by law.
- Where the personal information is public and exempted from coverage under applicable data protection laws.
- To seek advice from our lawyers and other professional advisors.
- To professional advisors (e.g. bankers, lawyers, accountants) and potential buyers and vendors in connection with the sale, disposal or acquisition by use of a business or assets.

Access to Personal Information We Collect

To the extent access is required by applicable law, you can ask to see the personal information that we hold about you. If you want to review, verify or correct your personal information, please submit a request to hr@regiotels.com.

When requesting access to your personal information, please note that we may request specific information from you to enable us to confirm your identity and right to access, as well as to search for and provide you with the personal information that we hold about

you. We may, in limited circumstances, charge you a fee to access your personal information; however, we will advise you of any fee in advance.

We reserve the right not to grant access to personal information that we hold about you if access is not required by applicable law. There are also instances where applicable law or regulatory requirements allow or require us to refuse to provide some or all of the personal information that we hold about you. In addition, the personal information may have been destroyed, erased or made anonymous. In the event that we cannot provide you with access to your personal information, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

Correction of Collected Personal Information

We endeavor to ensure that personal information in our possession is accurate, current and complete. If an individual believes that the personal information about him or her is incorrect, incomplete or outdated, he or she may request the revision or correction of that information. We reserve the right not to change any personal information we consider to be accurate or if such correction is not required by applicable law.

Retention of Collected Information

Except as otherwise permitted or required by applicable law or regulatory requirements, we may retain your personal information only for as long as we believe it is necessary to fulfill the purposes for which the personal information was collected (including, for the purpose of meeting any legal, accounting or other reporting requirements or obligations) and for IT archival purposes.

Personal data for data subjects in the European Union is by default erased by RegiÔtels after termination of your employment, with the exception of certain types of personal data, which may be stored for an extended period of time due to administrative purposes, e.g. for payment of retirement income or for giving references to other employers, or where such personal data must be retained to comply with regulatory requirements.

You may request that we delete the personal information about you that we hold, provided that we reserve the right not to grant such request if we are not required to delete personal information under applicable law. There are instances where applicable law or regulatory requirements allow or require us to refuse to delete this personal information. In the event that we cannot delete your personal information, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

Requests to Access, Delete, or Correct Information

Please send requests to access, delete, or correct your personal information to hr@regiotels.com.

Any request by you to us to delete your personal information will not result in deletion of any information submitted by you to a Third-Party provider. If you require the Third-Party to delete any of your personal information, you must contact the Third-Party directly to request such deletion.

As stated previously, there are instances where applicable law or regulatory requirements allow or require us to refuse to delete this personal information. In the event that we cannot delete your personal information, we will inform you of the reasons why, subject to any legal or regulatory restrictions.

Resolving Concerns

If you have questions or concerns regarding the handling of your personal information, please contact hr@regiotels.com. Alternatively, you may report concerns or complaints to the Managing Director.

Changes to Privacy Policy

We may change this Privacy Policy at any time by posting notice of such a change in the revision table below. The effective date of each version of this Privacy Policy is identified the revision table.

Security of Collected Information

We are committed to protecting the security of the personal information collected, and we take reasonable physical, electronic, and administrative safeguards to help protect the information from unauthorized or inappropriate access or use.

Additional Rights

You may also have the following additional rights, subject to certain exceptions and limitations as specified in applicable law:

Data portability

Where we are relying upon your consent or the fact that the processing is necessary for the performance of a contract to which you are party as the legal basis for processing, and that personal information is processed by automatic means, to the extent provided under applicable law, you have the right to receive all such personal information which you have provided to RegiÔtels in a structured, commonly used and machine-readable

format, and also to require us to transmit it to another controller where this is technically feasible;

Right to restriction of processing

You have the right to restrict our processing of your personal information where:

- You contest the accuracy of the personal information until we have taken sufficient steps to correct or verify its accuracy;
- Where the processing is unlawful, but you do not want us to erase the information;
- Where we no longer need the personal information for the purposes of the processing, but you require them for the establishment, exercise or defense of legal claims; or
- Where you have objected to processing justified on legitimate interest grounds (see below) pending verification as to whether RegiÔtels has compelling legitimate grounds to continue processing.

To the extent required by applicable law, where personal information is subjected to restriction in this way we will only process it with your consent or for the establishment, exercise or defense of legal claims.

Right to withdraw consent

Where we are relying upon your consent to process data, you have the right to withdraw such consent at any time. You can do this by contacting hr@regiotels.com.

Right to object to processing justified on legitimate interest grounds

Where we are relying upon legitimate interest to process data, then you have the right to object to such processing, and we must stop such processing unless we can either demonstrate compelling legitimate grounds for the processing that override your interests, rights and freedoms or where we need to process the data for the establishment, exercise or defense of legal claims. Normally, where we rely upon legitimate interest as a basis for processing we believe that we can demonstrate such compelling legitimate grounds, but we will consider each case on an individual basis.

You also have the right to lodge a complaint with a supervisory authority, in particular in your country of residence, if you consider that the processing of your personal data infringes this regulation.

Data Retention Policy

	Documents / Data processing purposes	Recommended Retention Period / beginning of Retention Period	Data subject	Types of personal data	Format	Legal reference	Comment(s)
Human Resources	Employment contract, data related to identification, administration and organization	**10 years** from the closure of the Fniancial Year during which the employment contract ended	Employees	Name data Contact data Special categories	Original or Electronic Format	No legal text	
	Pay slips	**10 Years** from the date of issuance	Employees	Name data Contact data Special categories	Original or Electronic Format	No legal text	
	Payroll data (taxes, social security, extra hours, bonus, expenses, advantage in kind)	**10 Years** from the closure of the FY during which the employment contract ended	Employees	Name data Special categories Health data Financial data	Original or Electronic Format	No legal text	
	Employee performance review information (assessment interview, copies of diplomas/qualifications, promotions)	Duration of the contractual relationship	Employees	Name data Special categories Assessment data	Original or Electronic Format	Art. 53 & 174 of the GDPR Recommendation CNIL n°2005-002	Recommendation CNIL n°2005-002: Date of termination
	Recruitment data not resulting in candidate's hiring (contract, CV, etc.)	**Duration of the recruitment phase**	Candidates	Name Data CV information Candidate assessment	Original or Electronic Format	Art. 5 & 17 GDPR	**2 years** from the last date of contact with the candidate
	Documents related to collective employment law matters (employee representation, collective bargaining agreements, etc.)	**Date of termination**	Employees	Name data Special categories	Original or Electronic Format	Art. 5 & 17 GDPR, Recommendation CNIL n°2005-002	
	Documents related to employee sick and maternity leaves	**5 Years** from the expiry of the year during which contributions were paid	Employees		Original or Electronic Format	Art. 10 Law of 27 November 1933 on social contributions	Duration of the limitation period for social security contributions
Business	Partners (suppliers, subcontractors, data processors)	**10 Years** from the end of the contractual relationship	Suppliers	Name data, Contact data, Financial Data	Original or Electronic Format	Art. 5 & 17 GDPR, Art. 14, 16, 189 CCom	Commercial correspondence is regarded in principle as accounting & financing document supporting documents, they must be kept for **10 years** from the closure of the relevant Financial Year (Art. 14 and 16 CCom)
	Commercial agreements and related documents/agreements with clients, suppliers, subcontractors non-disclosure agreements, etc.	**10 Years** From the end of contract/end of performance	Clients / Suppliers	Name data Contact data Financial data	Original or Electronic Format	Art. 14, 16 and 189 CCom	If the commercial agreements are regarded in principle as accounting & finance document supporting documents, the retention period is 10 years from the closure of the relevant Financial Year (Art. 14 and 16 CCom)
	Commercial correspondence (mail/email received and copies of mail/email sent) with clients, suppliers, sub-contractors, etc.	**10 Years** from the end of contract/end of performance	Clients / Suppliers	Name data Contact data Financial data	Original or Electronic Format	Art. 14, 16 and 189 CCom	The commercial correspondence is regarded in principle as accounting & finance document supporting documents, the retention period is 10 years from the closure of the relevant Financial Year (Art. 14 and 16 CCom)

Financial	Accounting & finance documents (general ledgers, financial statements, audit reports, P&Ls, etc.), including supporting documents and related correspondence in case of investigation or monitoring by the tax administration	**10 Years** from the closure of the relevant Financial Year	Employees Clients Suppliers	Name data Contact data Financial data	Original or Electronic Format	Art. 14, 16, 189 CCom, Art. § 162 (8) AO	
	Bank documents (account statements, etc.)	**10 Years** from the end of the Financial Year during which it was issued	Employees / Clients / Suppliers	Financial Data - Bank account details	Original or Electronic Format	Art. 14, 16, 189 CCom	The bank statements are regarded in principle as accounting & finance supporting documents, the retention period is 10 years from the closure of the relevant Financial Year
	Tax returns and documentation for inter-group pricing policies	**10 Years** from the end of the year in which the last transaction was registered in the books and records, or the commercial documents or other documents were established.	Employees / Clients / Suppliers	Name data Financial data	Original or Electronic Format	Art. § 162(8) and Art. §171 AO	
	VAT registry for the delivery or acquisition of goods or services within the EU, import/export documents related to the VAT	**10 Years** from the closure of the Financial Year for book-keeping & the date of issuance for other documents	N/A	N/A	Original or Electronic Format	Art. 65 VAT Law	
Administration	Invoicing information (including payment collection information and external dunning (judicial procedure)	**10 Years** from the closure of relevant Financial Year	Clients / Suppliers	Name data Contact data Financial data Metering	Original or Electronic Format	Art. 14, 16 and 189 CCom	
	Payment of suppliers	From the closure of the relevant FY	Suppliers	Name data Contact data Financial data	Original or Electronic Format	Art. 14, 16 and 189 CCom	
	Corporate documents (shareholder register, minutes of board, committee and shareholder meetings, among others)	**5 Years** from the loss of legal personality/striking from commercial register published in the official gazette2	Employees	Name data Contact data Financial data	Original or Electronic Format	Art. 1100-15 n°1, 1400-6 of the 1915	Corporate documents are regarded in principle as accounting & financing document supporting documents of the, the retention period is extended to **5 years** from the closure of the relevant Financial Year (Art. 14 and 16 CCom)
	Official documents related to company business activity (title of intellectual property rights, licenses, permits and authorizations, among others)	**10 Years** from the extinction of the rights or the loss of legal personality	Employees	Name data Financial data	Original or Electronic Format	Art. 14, 16, 189 CCom	The commercial correspondence are regarded in principle as accounting & financing document supporting documents, the retention period is 10 years from the closure of the relevant Financial Year (Art. 14 and 16 CCom)
	Commercial lease	**10 Years** from the end of the contract	Lessor	Name data Contact data Financial data	Original or Electronic Format	Art. 5 GDPR	The commercial leases are regarded in principle accounting & finance document as supporting documents, the retention period is **10 years** from the closure of the relevant Financial Year (Art. 14 and 16 CCom)
	Insurance contracts	**10 Years** from the end of a contract	Employees / Clients / Suppliers	Name data Contact data Financial data	Original or Electronic Format	Art. 44 of the Law of 27 July 1997 on insurance contracts	The insurance contracts are regarded in principle as accounting & finance document supporting documents, the retention period is 10 years from the closure of relevant Financial Year (Art.14 and 16 CCom)

Office	Building visitor registration	**3 months** following the end of the visit	Visitors	Name data Contact data	Original or Electronic Format	Arts. 5 & 17 GDPR Deliberation CNPD n° 64/2007	
Litigation	Litigation files	Statutes of limitations for civil or criminal actions (**30 years** for civil litigation **10 years** for commercial litigation) From the closure of the Financial Year during which the litigation terminated	Employees / Clients / Suppliers	Name data Contact data Financial data	Original or Electronic Format	Art. 2262 Cciv, Art. 14, 16, 189 CCom	In case the litigation files are regarded in principle as accounting & finance document supporting documents
Website	Cookies	Duration of navigation min. **13 months** from the acceptance of the cookie policy, subject to certain exemptions	Website users	Electronic identification data Behavioral data	Original or Electronic Format	Arts. 5 & 17 GDPR Recommendation CNIL n°2013-578 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (the "**e-privacy Directive**")	
Subscribers	Call detail Records	**5 Years** from the date of the recording or **customer request**	Customer's subscribers	Electronic identification data Behavioral data	Original or Electronic Format	Law of 24 July 2010 on electronic communications & Art.5 Law of 30 May 2005 on electronic communications (as amended by the Law of 24 July 2010)	Law of 24 July 2010 & Art. 5 Law of 30 May 2005: the traffic data related to electronic communication must be retained for 6 months by any service provider or operator processing subscriber and user traffic data.
	Subscriber Feed	**5 Years** from the date of the recording or **customer request**	Customer's subscribers	Name data Contact data Electronic identification data Behavioral data	Original or Electronic Format	Grand Ducal Regulation of 24 July 2010 on electronic communications	
	Location data	5 years or **customer request (6 months min.)** from the date of the recording	Customer's subscribers	Name data Contact data Electronic identification data Behavioral data	Original or Electronic Format		Grand-Ducal Regulation of 24 July 2010 defines the data to be retained, including the data necessary to trace
	Transaction data records	6 months min. from the date of the recording	Customer's subscribers	Electronic identification data Behavioral data	Original or Electronic Format		
	Community	**1 Year** following the date of the recording	Customer's subscribers	Name data Contact data Financial data	Original or Electronic Format		
	Digital identity	**6 months min**. from the date of the recording	Customer's subscribers	Name data Contact data	Original or Electronic Format		
	Tickets resolution and litigation	**30 days** from the resolution of the ticket, once any applicable mandatory legal retention period is over	Customer's subscribers	All personal data listed in this table	Original or Electronic Format		
Personal data protection	Data on the appointment of a DPO	**1 Year** from the date the data controller or the sub-contractor, having made the appointment, informs the CNPD of the new appointment and/or the termination of the appointed DPO's position.	Any person	Name data Contact data	Original or Electronic Format		
	Information request to the National Commission for Data Protection	**3 Years** from the closing of the file related to the request	Any person	Name data Contact data	Original or Electronic Format	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 data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)	
	Claims management	**10 Years** from the closing of the file	Any person who is a victim of a personal data breach/violation	Name data Contact data	Original or Electronic Format		
	Notification of the violation to the National Commission for Data Protection	**10 Years** from the closing of the file	Person reporting the breach/ violation and data controller's contact person	Name data Contact data	Original or Electronic Format		

1 The retention policy is applicable to the period during which the legal entity, contract, title, title of property, etc., is in force, plus the recommended retention period (RP) indicated in the table.

2 The application of a 2-month buffer on all retention periods might be considered occurring on the publication date of the closure of the liquidation of the legal entity concerned.

For the purposes of clarification, if and when a contractual relationship with RegiÔtels is terminated, the data is removed from the RegiÔtels servers within two months of the end date. In line with clause 4(d), prior to deletion, an extraction of relevant data is made and stored on an external hard drive for which there is also a backup copy kept. Only the data Protection Officer has access to either the external hard-drive or its backup.

4 Art. 5 of the GDPR: personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

5 Art. 17 of the GDPR: Personal data shall be subject to erasure by the data controller when no longer necessary in relation to the purposes for which it was collected or processed.

In the absence of specific Luxembourg regulation, the CNPD will, in practice, frequently follow the recommendations issued by the CNIL.

The limitation period for the establishment of the tax and payment of the tax is 5 years (Art. 144 AO and Art. 81 VAT Law) from the end of Financial Year declared and begins to run at the end of the year that gave rise to the tax claim.

However, in case of a non-filing of a return or in case of additional taxation for incomplete or incorrect return, with or without fraudulent intent, the limitation period is 10 years for direct taxation (Art.10 of the Law of 27 November 1933).

Please note that pursuant to Article § 162(8) AO, the books, records, and, inasmuch as they are relevant for the taxation, the corporate documents and other documents shall be kept for a period of 10 years starting at the end of the calendar year in which the last transaction was registered in the books and records, or the commercial documents or other documents were established.

Data Subject Consent & Withdrawal Form

Data Subject Consent Form

GDPR consent statement 1.1

I, [data subject name], hereby grant RegiÔtels International Sàrl and [third-party processor] authority to process my personal data for the purpose of [specify in explicit terms, the legitimate reason for processing the personal data], which is attached to this declaration.

GDPR consent statement 1.2

I am aware that I may withdraw my consent at any time by using form – Data Subject Consent Withdrawal Form (attached below).

Signed by data subject:

Date:

Request actioned by on behalf of RegiÔtels:

Date:

Data Subject Consent Withdrawal Form

I, [data subject name], withdraw my consent to process my personal data from RegiOtels International Sàrl. RegiOtels International Sàrl no longer has my consent to process my personal data for the purpose of [specify legitimate reason of processing personal data], which was previously granted.

Signed by data subject:

Date:

Request actioned by:

Date:

DPIA Assessment and Register

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and should be read alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs. For more information on how and why to fill in this form, please consult here.

You should start to fill out the template at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated back into your project plan.

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated reduced accepted	Low medium high	Yes/no

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA

Supplier Data Processing Agreement

This agreement is entered between:

1. RegiOtels International Sàrl, a limited liability company, with registered address at 2 rue de la Chapelle, L-1325, Luxembourg, and registration number B232714
(hereinafter

“**Processor**”);and

2. _____, with registered address at

_____

with company registration number _____

(hereinafter “**Controller**”);

hereinafter collectively referred to as "**parties**" and separately "**party**",

Introduction

1. The Processor is a software service provider;
2. The Controller has access to the personal data of various customers;
3. The Controller and the Processor are a party to one or more contracts (hereinafter "**Service Agreement**") that involve the processing of personal data by the Processor for the benefit of the Controller;
4. The Parties wish to supplement the Service Agreement with the provisions below with respect to processing of personal data in accordance to the General Data ProtectionRegulation EU 2016/679.

Now, therefore, in consideration of the foregoing, it is agreed as follows:

1. The parties agree to perform all their rights and obligations under this Agreement (including,without limitation, the collection, use, processing, transfer, storage and

maintenance of personal data) in accordance with the EU Directive 95/46 and implementing local laws, as maybe amended, replaced or repealed from time to time, including, as of 25 May 2018, by the General Data Protection Regulation EU 2016/679, as well as supplementing national laws (hereinafter "**Data Protection Laws**"). For the purposes of this Agreement, "personal data", "process/processing", "data subject", "data controller", "data processor", and "subprocessor"shall have the same meaning as defined under applicable Data Protection Laws.

2. Each party agrees to comply with its respective obligations as data controller and/or as data processor or subprocessor in accordance with the applicable Data Protection Laws for the performance of and in connection with the Service Agreement.
3. If and where the Processor processes personal data on behalf of the Controller, it shall:
    - ensure that the personnel authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
    - not transfer personal data outside the European Economic Area (“EEA”), except in accordance with the Controller’s instructions and EU Commission's decisions finding that certain non-EEA countries provide an adequate level of protection or another appropriate data transfer mechanisms such as EU Commission Standard ContractualClauses;
    - use the personal data exclusively for the purpose of carrying out its obligations under the Service Agreement and treat the personal data confidentially;
    - without undue delay notify the Controller of any discovered or suspected personal data breaches;
    - implement all appropriate technical and organizational measures to protect personaldata;
    - assist the Controller by providing information and cooperation in case of data subjectaccess requests relating to Controller Data that is or has been processed by the Processor.
4. For the purposes and subject to the conditions of this Agreement, the Controller authorizes the Processor to subcontract all or part of the processing to other (sub)processors (“**Subprocessor**”), provided that the applicable requirements set forth in the applicable DataProtection Laws and this Agreement are complied with at all times, specifically to theSubprocessor(s).
5. As long as the Service Agreement is in place, this Agreement will remain relevant.

Save as otherwise agreed herein, termination rights and requirements shall be the same as set forth in the Service Agreement.

6. Upon termination of the Service Agreement, the Processor shall destroy or return thepersonal data to Controller. To this end, the Controller is to notify Processor, within a maximum delay of ten (10) working days by reliable means whether the personal data provided are to be returned or deleted.

7. This Agreement will be governed by the laws of Luxembourg. Any disputes arising out of thisAgreement will be solved by the competent court in Luxembourg.

The present Agreement has been executed in Bruges on__/_____/ _____in two (2)originals where both parties have taken one each.

Data Breach Response and Notification Procedure

Version:	1.0
Date of version:	February 2022
Confidentiality level:	External Use

Change history

Date	Version	Created by	Description of change
February 2022	1.0	Gregory Tugendhat	Created document

1. Scope, purpose and users

This Procedure provides general principles and approach model to respond to, and mitigate breachesof personal data (a “personal data breach”) in one or both of the following circumstances:

- The personal data identifies data subjects who are residents of the Member States of theEuropean Union (EU) and countries in the European Economic Area (EEA), regardless of where that data is subject to processing globally; and
- The personal data is subject to processing in the EU and/or EEA, regardless of the country ofresidency of the data subject.

The Procedure lays out the general principles and actions for successfully managing

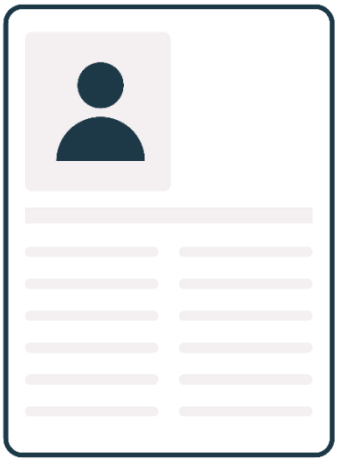
the response to a data breach as well as fulfilling the obligations surrounding the notification to Supervisory Authorities and individuals as required by the EU GDPR.

All Employees/Staff, contractors or temporary Employees/Staff and third parties working for or acting on behalf of IRIS Connect ("Company") must be aware of, and follow this Procedure in the event of a personal data breach.

2. Reference documents

- EU GDPR 2016/679 (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 data and on the free movement of such data, and repealing Directive 95/46/EC).
- Personal Data Protection Policy.

3. Definitions



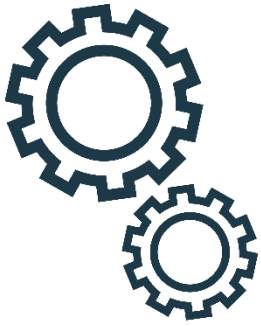
The following definitions of terms used in this document are drawn from Article 4 of the European Union's General Data Protection Regulation (GDPR):

"Personal Data" means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person Regulation.

"Controller" is the natural or legal person, public authority, agency or any other body, which alone or jointly with others, determines the purposes and means of the processing of personal data.

“Processor” is a natural or legal person, public authority, agency or any other body which processes personal data on behalf of a Data Controller.

“Processing” means any operation or set of operations which is performed on personal data or on sets of personal data, whether 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.



“Personal Data Breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

“Supervisory Authority” means an independent public authority which is established by a Member State pursuant to Article 51.

4. Data Breach Response Team

A Data Breach Response Team must be a multi-disciplinary team comprised of knowledgeable and skilled individuals in IT Department, IT Security, Legal, Legal and Public Affairs The team may be a physical (local) or virtual (multiple locations) team which responds to any suspected/alleged personal data breach. For the RegiÔtels Response Team, please refer to digital@regiotels.com

The Financial Director appoints the members of the Data Breach Response Team. The Team must be appointed regardless of whether or not a breach has occurred.

The team must ensure that necessary readiness for a personal data breach response exists, along with the needed resources and preparation (such as call lists, substitution of key roles, desktop exercises, plus required review of company policies, procedures and practices).

The team's mission is to provide an immediate, effective, and skilful response to any suspected/alleged or actual personal data breaches affecting the Company.

If required, the team members may also involve external parties (e.g. an information security vendor for carrying out digital forensics tasks or an external communications agency for assisting the Company in crisis communications needs.

The Data Breach Response Team Leader can choose to add additional personnel to the team for the purposes of dealing with a specific personal data breach.

The Data Breach Response Team may deal with more than one suspected/alleged or actual personal data breach at a time. Although the core team may be the same for each suspected/alleged or actual personal data breach, there is no requirement for this.

The Data Breach Response Team must be prepared to respond to a suspected/alleged or actual personal data breach 24/7, year-round. Therefore, the contact details for each member of the Data Breach Response Team, including personal contact details, shall be stored in a central location, and shall be used to assemble the team whenever notification of a suspected/alleged or actual personal data breach is received.

5. Data Breach Response Team duties

Once a personal data breach is reported to the Data Breach Response team leader, the team must implement the following:

- Validate/triage the personal data breach
- Ensure proper and impartial investigation (including digital forensics if necessary) is initiated, conducted, documented, and concluded
- Identify remediation requirements and track resolution
- Report findings to the top management
- Coordinate with appropriate authorities as needed

- Coordinate internal and external communications
- Ensure that impacted data subjects are properly notified, if necessary

The Data Breach Response Team will convene for each reported (and alleged) personal data breach, and will be headed by the Data Breach Response Team Leader.

6. Data Breach Response process

The Data Breach Response Process is initiated when anyone who notices that a suspected/alleged or actual personal data breach occurs, and any member of the Data Breach Response team is notified. The team is responsible to determine if the breach should be considered a breach affecting personal data.

The Data Breach Team leader is responsible for documenting all decisions of the core team. Since these documents might be reviewed by the supervisory authorities, they need to be written very precisely and thoroughly to ensure traceability and accountability.

7. Personal data breach notification: Data processor to data controller

When the personal data breach or suspected data breach affects personal data that is being processed on behalf of a third party, the Data Protection Officer of the Company (the Financial Controller) acting as a data processor must report any personal data breach to the respective data controller/controllers without undue delay.

The Data Protection Officer will send Notification to the controller that will include the following:

- A description of the nature of the breach
- Categories of personal data affected
- Approximate number of data subjects affected
- Name and contact details of the Data Breach Response Team Leader/ Data

Protection Officer.

- Consequences of the personal data breach
- Measures taken to address the personal data breach
- Any information relating to the data breach

DPO will record the data breach into the Data Breach Register.

8. Personal data breach notification: Data controller to supervisory authority

When the personal data breach or suspected data breach affects personal data that is being processed by the Company as a data controller, the following actions are performed by the Data Protection Officer:

The Company must establish whether the personal data breach should be reported to the Supervisory Authority.

1) In order to establish the risk to the rights and freedoms of the data subject affected, the Data Protection Officer must perform the Data Protection Impact Assessment on the processing activity affected by the data breach.
2) If the personal data breach is not likely to result in a risk to the rights and freedoms of the affected data subjects, no notification is required. However, the data breach should be recorded into the Data Breach Register.
3) The Supervisory Authority (CNPD – databreach@cnpd.lu) must be notified with undue delay but no later than in 72 hours with the form attached in annex, if the personal data breach is likely to result in a risk to the rights and freedoms of the data subjects affected by the personal data breach. Any possible reasons for delay beyond 72 hours must be communicated to the Supervisory Authority.

DPO will send Notifications to the Supervisory Authority that will include the following:

- A description of the nature of the breach

- Categories of personal data affected
- Approximate number of data subjects affected
- Name and contact details of the Data Breach Response Team Leader/ Data Protection Officer
- Consequences of the personal data breach
- Measures taken to address the personal data breach
- Any information relating to the data breach

9. Personal data breach notification: Data controller to data subject

The Financial Director must assess if the personal data breach is likely to result in high risk to the rights and freedoms of the data subject. If yes, the Data Protection Officer the Company must notifywith undue delay the affected data subjects.

The Notification to the data subjects must be written in clear and plain language and must containthe same information listed in Section 7.

If, due to the number of affected data subjects, it is disproportionately difficult to notify each affected data subject, the Data Protection Officer must take the necessary measures to ensure thatthe affected data subjects are notified by using appropriate, publicly available channels.

10. Accountability

Any individual who breaches this Procedure may be subject to internal disciplinary action (up to andincluding termination of their employment); and may also face civil or criminal liability if their actionviolates the law.

11. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time
Call lists & substitution	Microsoft One-drive of Data breach response teamleader	Data breach response team leader	Only authorized persons can edit the files	Permanently
Contact details	Microsoft One-drive of Data breach response teamleader	Data breach response team leader	Only authorized persons can edit the files	Permanently
Documented decisions of the Data Breach Response Team	Microsoft One-drive of Data breach response teamleader	Data breach response team leader	Only Data Breach Response Team leader can edit the files	5 years
Data breach notifications	Microsoft One-drive of Data breach response teamleader	Data breach response team leader	Only Data Breach Response Team leader can edit the files	5 years
Data Breach Register	Microsoft One-drive of Data breach response teamleader	Data Protection Officer	Only Data Protection Officer can edit the files	Permanently

12. Validity and document management

This document is valid as of February 2022.

The owner of this document is the Data Protection Officer who must check and, if necessary, updatethe document at least once a year.

Data Protection Officer

Gregory Tugendhat

[signature]

Data Breach Register

This document registers the time and date of each data breach and the time for notification to the authorities via the email address: databreach@cnpd.lu

The completion of this form is the responsibility of the Data Protection Officer

Time & Date of Data Breach	Comments on the Data Breach	Actions taken	By Whom	Time & Date of Notification to CNPD	Signtature of Data Protection Officer

Data Breach Notification Form to the Supervisory Authority

Please return this form **in its docx version** to the email address: databreach@cnpd.lu

(**Attention:** Do not transmit the personal data concerned by the data breach with the notification of the violation to the CNPD)

Data breach notification

Preliminary or complementary notification	☐ Preliminary ☐ Complete ☐ Complementary / amended notification -> In case of complementary / amended notification, enter here the notification number provided by the CNPD
Summary of data breach *(Explain what has happened, what has not worked and how it happened)*	Click or tap here to enter text.

Identification of stakeholders

1.1 The controller	
Name of the Organization	Click or tap here to enter text.
Address and contact details of the Organization	Click or tap here to enter text.
Sector of activity of the Organization	Click or tap here to enter text.
Number of employees of the Organization	☐ < 10 ☐ < 50 ☐ < 250 ☐ < 1000 ☐ ≥ 1000

1.2 The declarer	
Name and function of the declarer	Click or tap here to enter text.
Address and contact details of the declarer	Click or tap here to enter text.

1.3 involvement of others parties, except the controller, in the data breach	
Name (s) and description of the other parties involved	Click or tap here to enter text.

Chronology

Specify date and time specific format « JJ/MM/YY HH:MM »

Beginning date of the breach	Click or tap to enter a date.
Date of awareness of breach *(by the controller or the processor)*	Click or tap to enter a date.
Ending date of breach	Click or tap to enter a date.
Reason of a late breach notification *(when there is more than 72 hours between awareness and notification)*	Click or tap here to enter text.
Comments on dates / hours	Click or tap here to enter text.

About the breach

How was the breach detected?	Click or tap here to enter text.
Nature of the incident	Select an item (Without modifying it) Click or tap here to enter text.
Cause of the breach	Select an item (Without modifying it)

About the data affected by the breach

Regular data	☐ Data subject identity (name, surname, date of birth) ☐ National identification number ☐ Contact details ☐ Identification data ☐ Economic and financial data ☐ Official documents ☐ Location data List the concerned data : Click or tap here to enter text.
Special categories of data or related to convictions / offences	☐ Data revealing racial or ethnic origins ☐ Political opinions ☐ Religious or philosophical beliefs ☐ Trade union membership ☐ Sex life data ☐ Health data ☐ Criminal convictions, offence or security measures ☐ Genetic or biometric data ☐ Not yet known List the concerned data : Click or tap here to enter text.

About the data subjects

Type	Select an item (Without modifying it)
Detailed description of the data subjects	Click or tap here to enter text.
Number of data subjects	Click or tap here to enter text.
Country of residence of the data subjects	Click or tap here to enter text.

Risk analysis

7.1 Impact

Loss of confidentiality	☐
Loss of integrity	☐
Loss of availability	☐

Nature of the potential impact on the data subjects	Select an item (Without modifying it) Explanations related to the impact's nature : Click or tap here to enter text.

7.2 Probability

Assessment of the probability that the potential risk materializes	Click or tap here to enter text.

7.3 Conclusion – risk

Assessment of the level of risk to the rights and freedoms of the data subjects	Select an item (Without modifying it)
Detail the reasoning that has led you to this assessment *(a risk analysis can be transmitted in attachment)*	Click or tap here to enter text.

Measures related to the incident

8.1 Measures in place before the violation	
Description of the technical and organizational measures	Click or tap here to enter text.

8.2 Measures taken to limit the potential impact of the violation on the data subjects	
Description of the technical and organizational measures	Click or tap here to enter text.

8.3 Measures to inform the persons concerned (*fill the boxes A) OR the box B)*)	
A) You have or are going to inform (*within the meanings of the art. 34*) the data subjects	
Information to the data subjects	Date of information: Click or tap to enter a date. Number of informed people: Click or tap here to enter text. Channel used to inform: Click or tap here to enter text. *(Ex: mail, email, phone ...)*
Content of the information provided to the data subjects	Click or tap here to enter text. *(Documents can be passed using an attachment if necessary)*

Recommendations given to data subjects in order to protect themselves	Click or tap here to enter text.
B) You will not inform the data subjects	
Reason not to inform the concerned persons	Click or tap here to enter text.

8.4 Measures taken to prevent the violation from recurring	
Description of the technical and organizational measures	Click or tap here to enter text.

Measures related to the incident

Is this notification a cross-border notification made to your lead supervisory authority?	☐Yes ☒ No If yes, precise list of EU countries concerned by the breach: Click or tap here to enter text.
Has the breach been or will it be notified directly to other concerned EU supervisory authority?	☐Yes ☒ No If yes, indicate the other(s) Supervisory Authority concerned: Click or tap here to enter text.
Has the breach been or will it be notified to Data Protection Authorities outside the EU ?	☐Yes ☒ No If yes, indicate the other(s) Data Protection Authority outside EU concerned: Click or tap here to enter text.
Has the breach been or will it be notified to other EU regulators because of other legal obligations (example: NIS directive, eIDAS regulation)?	☐Yes ☒ No If yes, indicate the other(s) regulator(s) notified: Click or tap here to enter text.

RegiÔtels

You look after the guest,
we look after the rest

GDPR COMPLIANCE MANUAL

regiotels.com