

Techryt BPO Global Privacy Policy

Last updated: July 2026

Techreet SARL (operating as Techryt BPO) · Lebanon · GCC · Europe · USA

1. Introduction

This Global Privacy Policy ("Policy") explains how Techreet SARL, operating as Techryt BPO ("Techryt", "we", "us", or "our") collects, uses, discloses, and protects personal data in connection with:

- our business process outsourcing (BPO) services, including outbound and inbound contact centre, customer support, CRM operations, back-office support, and related customer engagement;
- our AI products and software tools that sit beside client teams;
- our creative and digital services (including development, UI/UX, social media management, and graphic design);
- our websites, talent pool, online services, and chat experiences; and
- our business operations.

Techryt is operated by Techreet SARL, a company established in Lebanon, with a US-registered counterpart, and provides services to clients across the GCC, Europe, the USA, and other jurisdictions.

We recognize the importance of privacy and data protection and are committed to complying with applicable data protection laws globally, including, where applicable, the European Union and United Kingdom General Data Protection Regulation (collectively, "GDPR"), the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA/CPRA"), Brazil's Lei Geral de Protecao de Dados ("LGPD"), South Africa's Protection of Personal Information Act ("POPIA"), relevant Gulf cooperation frameworks and UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data ("UAE PDPL"), and other similar laws, as well as relevant Lebanese data protection provisions (including Law No. 81 of 2018 on Electronic Transactions and Personal Data).

2. Scope of this Policy

This Policy applies to:

- Personal data we process in our capacity as a controller, including:
 - personal data of visitors to our websites and online services;
 - personal data of individuals who contact us, use our chatbot, or inquire about our services;
 - personal data of candidates who submit profiles to our talent pool;
 - personal data of individuals with whom we communicate directly about our own services (for example, prospects, vendors, and business partners);
 - personal data of our employees, contractors, and applicants (where we choose to apply this Policy in addition to specific employment notices).
- Personal data we process in our capacity as a processor (or service provider/processor under certain laws) on behalf of our clients, when we:
 - conduct outbound or inbound campaigns, support, CRM, or back-office work using contact lists and instructions provided by clients;
 - record or monitor calls or interactions, where permitted by law and as instructed by clients;
 - operate AI products or quality tools on client data under client instructions;
 - provide reports, analytics, and other deliverables to our clients.

When we act as a processor or service provider, we process personal data on behalf of and under the instructions of our clients, who act as controllers or businesses. In those cases, our clients' privacy policies and notices will also apply, and individuals should refer to those notices for further details about how their personal data is handled.

This Policy does not apply to the personal data of our employees and staff where a separate internal privacy notice is provided, except where explicitly stated.

3. Controller and Contact Details

For processing activities where Techryt acts as a controller, the controller is:

Techreet SARL (operating as Techryt BPO)

Lebanon

Email: info@techryt.com

Website: <https://techryt.com>

Depending on where you reside, you may also have the right to lodge a complaint with a supervisory authority or data protection regulator, as described in Section 13 below.

If we are acting as a processor or service provider on behalf of a client, that client will be the controller (or equivalent term under local law) responsible for your personal data.

4. Key Definitions

For the purposes of this Policy:

- "Personal data" (or "personal information") means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, online identifier, or one or more factors specific to that person.
- "Processing" means any operation or set of operations performed on personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, alignment, combination, restriction, erasure, or destruction.
- "Controller" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "Processor" means a natural or legal person which processes personal data on behalf of the controller.

Other terms used in this Policy have the meanings given to them under applicable data protection laws.

5. When Techryt Acts as Controller vs. Processor

5.1 Techryt as Controller

We act as a controller when we determine the purposes and means of processing personal data, such as when we:

- manage our relationship with clients, vendors, and business partners;
- operate our websites, talent pool, online portals, chatbot, and social media pages;
- conduct our own marketing and business development activities;
- recruit, onboard, and manage personnel, and evaluate talent-pool submissions;
- maintain suppression lists and do-not-contact lists for our own marketing.

5.2 Techryt as Processor or Service Provider

We act as a processor or service provider when we process personal data on behalf of and under the instructions of our

clients, such as when we:

- receive contact lists or customer databases from clients and use them to conduct outbound or inbound calling campaigns, email or messaging outreach, support queues, CRM work, or surveys;
- record and monitor calls or interactions, subject to applicable law, to provide quality assurance and reporting to clients;
- run AI products (for example debt-recovery or quality-assurance tooling) on client-provided data under client instructions;
- produce reports, dashboards, and analytics about campaign performance and customer engagement.

In these situations, our clients remain responsible for providing appropriate privacy notices to individuals and for choosing the lawful basis for processing. We enter into data processing agreements with our clients that govern such processing and include appropriate data protection obligations.

6. Categories of Personal Data We Process

The categories of personal data we process may include, depending on the context:

- Identification and contact data: name, title, employer, job role, email address, postal address, phone number(s), and similar identifiers.
- Demographic and relationship data: country of residence, language preferences, relationship history with our clients, customer segment.
- Communication data: call content, call recordings and transcripts (where permitted by law), chat messages, call metadata (time, duration, outcome), notes taken by our agents, and correspondence via email, SMS, messaging apps, or other channels.
- Marketing and preference data: marketing preferences, opt-in/opt-out records, subscription status, do-not-call/do-not-contact flags and suppression lists.
- Technical and usage data: IP addresses, device and browser information, cookies and similar technologies, log data, and usage data related to our websites, chatbot, or portals.
- Talent pool and recruitment data: CVs/resumes, professional history, qualifications, preferred tracks or roles, interview notes, and short audio introductions submitted through our talent pool (where applicable and permitted by law).
- Product and operations data: account or case identifiers provided by clients for AI products and BPO delivery, quality scores, and related operational metadata.

We generally do not seek to collect sensitive or special categories of personal data (such as health data, religious beliefs, or political opinions) in the course of our BPO campaigns. If such data is collected incidentally during a call or interaction, it is processed only as necessary and in accordance with applicable law and client instructions.

7. Sources of Personal Data

We may obtain personal data from the following sources:

- Directly from individuals, for example when they:
 - speak with our agents on the phone or via other communication channels;
 - fill in forms on our websites, talent pool, portals, or landing pages;
 - interact with our website chatbot;
 - communicate with us by email or other means.
- From our clients, who may provide us with:

- contact lists, customer databases, or lead lists;
 - historical interaction data and campaign-related information;
 - data required to operate AI products under their instructions.
- From publicly available sources, such as business directories, professional networking sites, or public websites, where permitted by law and consistent with our clients' instructions and our own legitimate interests.
- From service providers and partners, such as providers of dialers, CRM systems, cloud hosting, analytics, or other tools that support our campaigns and operations.

8. Purposes and Legal Bases for Processing

8.1 When Techryt is Controller

Where GDPR or similar laws apply, we rely on one or more of the following legal bases for processing:

- Performance of a contract: to enter into and perform contracts with our clients, vendors, and personnel, and to take steps at the request of the data subject prior to entering into a contract.
- Legitimate interests: to pursue our legitimate interests in managing and growing our business, including communicating with clients and prospects about our services; maintaining and improving our services and operations; evaluating talent-pool submissions for potential placement on client floors; ensuring network and information security; and protecting our rights, property, and interests, and those of our clients and staff.
- Consent: where required by law, for example, for certain marketing communications, use of cookies and similar technologies, or specific types of call or audio recording. When consent is our legal basis, individuals may withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.
- Compliance with legal obligations: to comply with applicable laws and regulations, including those related to record-keeping, accounting, tax, and responding to lawful requests from public authorities.

As controller, we may process personal data to operate, provide, and improve our websites, services, products, and operations; respond to inquiries; manage client, vendor, and partner relationships; conduct our own marketing and business development activities; manage recruitment, talent-pool, and HR processes; detect, prevent, and investigate fraud or security incidents; and comply with legal obligations and defend our legal rights.

8.2 When Techryt is Processor or Service Provider

When we act as a processor or service provider, we process personal data on behalf of and under the instructions of our clients, who are responsible for identifying an appropriate legal basis for the processing and providing any necessary notices or consents. Our processing on behalf of clients may include conducting sales, support, CRM, back-office, or survey campaigns; recording and monitoring interactions for quality assurance, training, and compliance; operating AI products under client instructions; managing opt-out and do-not-contact lists; and providing reports, analytics, and performance metrics.

9. International Data Transfers

Given the international nature of our services, personal data may be transferred to and processed in countries other than the one in which it was originally collected, including Lebanon and other countries where our clients, service providers, or partners are located across the GCC, Europe, the USA, and elsewhere. Some of these countries may have data protection laws that are different from (and may be less protective than) the laws of your country.

Where required by law, we take appropriate safeguards to ensure that personal data remains protected in accordance with this Policy and applicable data protection laws. These safeguards may include implementing Standard Contractual Clauses approved by the European Commission or equivalent mechanisms for transfers from the EEA or UK; ensuring that recipients are subject to adequate data protection obligations; and implementing additional technical and

organizational measures to protect the data.

10. Data Sharing and Recipients

We may share personal data with the following categories of recipients, where lawful and appropriate:

- Clients: where we act as a processor or service provider, we share personal data (including interaction results, recordings, and reports) with the client that engaged us. Where candidates join our talent pool, we may share relevant profile information with clients considering those candidates for their floors, consistent with the purpose of the talent pool.
- Service providers and sub-processors: third-party vendors who support our operations, such as providers of dialer and telephony systems, CRM and ticketing systems, cloud hosting, IT support, analytics, AI infrastructure, quality monitoring, and professional services.
- Professional advisers: lawyers, auditors, accountants, and consultants who provide professional services to us, subject to confidentiality obligations.
- Public authorities and regulators: government, regulatory, or law enforcement authorities where we are required or permitted by law to disclose personal data.
- Corporate transactions: in connection with any proposed or actual merger, acquisition, sale of assets, financing, restructuring, or similar transaction involving Techreet SARL or Techryt.

We do not sell personal information for monetary consideration, and we do not share personal information for cross-context behavioral advertising as those terms are defined under certain laws such as the CCPA/CPRA. If this changes, we will update this Policy and provide any required notices and choice mechanisms.

11. Data Retention

We retain personal data for as long as necessary to fulfill the purposes for which it was collected and to comply with our legal, contractual, and regulatory obligations. The criteria we use to determine retention periods include the duration of our contractual relationship with the relevant client, vendor, or individual; legal obligations to retain records; the existence of actual or potential disputes or legal proceedings; and our and our clients' operational needs, including maintaining suppression and do-not-contact lists.

Call recordings, campaign data, talent-pool submissions (including resumes and audio introductions), chatbot transcripts, and related information are typically retained for a period aligned with our operational needs and, where applicable, periods agreed with clients and set out in our contracts, after which they are securely deleted or anonymized, unless a longer retention period is required or permitted by law.

12. Security of Personal Data

We implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access. These measures may include access controls and role-based permissions; encryption and secure transmission protocols where appropriate; logical and physical security controls; regular training and awareness programs for staff; and incident detection, response, and notification procedures.

While we take reasonable steps to protect personal data, no system or transmission of data over the internet can be guaranteed to be completely secure.

13. Your Rights

Depending on your country or state of residence and applicable law, you may have certain rights in relation to your personal data. These may include the right of access; the right to rectification; the right to erasure; the right to restriction

of processing; the right to data portability; the right to object (including to direct marketing); rights relating to automated decision-making; and the right to withdraw consent where processing is based on consent.

13.1 Additional Rights for EEA and UK Residents

If you are located in the European Economic Area or the United Kingdom, you may also have the right to lodge a complaint with a supervisory authority, in particular in the Member State or country of your habitual residence, place of work, or where an alleged infringement has occurred.

13.2 Additional Rights for California and Certain US State Residents

If you are a resident of California or certain other US states that have enacted privacy laws, you may have additional rights, which may include the right to know, the right to delete, the right to correct, and the right to non-discrimination for exercising your privacy rights.

As noted above, we do not sell or share personal information in a way that would trigger a right to opt out of sale or sharing for cross-context behavioral advertising.

13.3 Additional Notes for GCC Residents

Where UAE PDPL or other Gulf data-protection rules apply, you may have rights of access, correction, erasure, and restriction, and the right to lodge a complaint with the competent supervisory authority, subject to applicable law.

13.4 Exercising Your Rights

To exercise your rights under applicable law, you may contact us using the details provided in Section 17. We may need to verify your identity before responding to certain requests. Where permitted by law, you may also designate an authorized agent to submit requests on your behalf.

We will respond to your request within the time period required by applicable law. When we process your personal data as a processor or service provider on behalf of a client, we may first refer your request to the relevant client, and we may cooperate with them to respond.

14. Cookies and Similar Technologies

We may use cookies, web beacons, and similar technologies on our websites and online services to enable essential functionality and security; remember your preferences and settings; analyze website traffic and usage patterns to improve our services; and support certain marketing and analytics activities.

Where required by law, we will obtain your consent before using non-essential cookies and provide you with information about the types of cookies we use and how to manage your preferences. You can typically configure your browser to refuse all or some cookies. However, if you disable or refuse cookies, some parts of our website may not function properly.

15. Children's Privacy

Our services and websites are not directed to children, and we do not knowingly collect personal data from individuals under the age required by applicable law without appropriate parental or guardian consent. If we become aware that we have collected personal data from a child contrary to this Policy or applicable law, we will take steps to delete that information as soon as practicable.

16. Automated Decision-Making and Profiling

We may use limited profiling and analytics in the context of our BPO, product, and customer engagement activities, for example to segment contact lists for campaigns based on objective criteria provided by clients; prioritize leads based on campaign performance indicators; support AI-assisted quality or outreach tools under client instructions; and analyze interaction outcomes and agent performance.

These activities are not intended to produce legal effects concerning individuals or similarly significantly affect them. We do not engage in fully automated decision-making that produces such effects without human involvement, unless permitted by law and subject to appropriate safeguards.

Talent-pool evaluation involves human review of submitted materials; automated tools, if used, assist screening and do not solely determine placement decisions without human involvement.

17. How to Contact Us

If you have any questions or concerns about this Policy or our processing of your personal data, or if you wish to exercise your rights, you may contact us at:

Techreet SARL (operating as Techryt BPO)

Lebanon

Email: info@techryt.com

Website: <https://techryt.com/contact>

When you contact us, please provide sufficient information to allow us to understand your request and verify your identity, where necessary.

18. Changes to this Policy

We may update this Policy from time to time to reflect changes in our practices, technologies, legal requirements, or other factors. When we make material changes, we will take appropriate steps to inform you, such as by posting a prominent notice on our website or by sending you a direct communication, and we will indicate at the top of the Policy when it was last updated.

Your continued use of our services or interaction with us after the effective date of an updated Policy will constitute your acknowledgment of the updated Policy.