BIRD PRIVACY STATEMENT

This privacy statement aims to provide clear, accessible, and easy-to-understand information to all website visitors, leads, customers, and the recipients of our communication services.

As an omnichannel communications platform, we and our Affiliates (together “we”, “us”, or “our”,) provide a wide range of solutions to improve the communications experience for developers, businesses, and your intended audience. In order to deliver these services, operate our websites, and to conduct our day-to-day business we process personal data. In this privacy statement, the terms “you”, “your”, or “Customer” refer to you. “Affiliate” means any entity that directly or indirectly controls, or is controlled by, or is under common control with the party specified. For purposes of this definition, “control” means direct or indirect ownership of more than fifty percent (50%) of the voting interests of the subject entity or the power to direct the management and policies of the subject entity.

The information contained in this privacy statement relates to the practices and services as provided by us.

This privacy statement applies to the use of our websites, the platform, and all products and services provided by us, and contains information about what personal data we collect, why we collect it, and how we process it so that you can make an informed decision before making use of our website, platform, and communications services.
Personal data refers to information that would allow any natural person to be directly or indirectly identified. Your use of our website, platform, or services may involve processing of personal data relating to three categories of individuals:

- Personal data related to website visitors in line with the settings applied in the cookie consent manager, or submitted by you through forms or other means.
- Personal data related to a customer or potential customer, referred to as “Customer Account Data” or “potential customer information”.
- Personal data related to an end-user or recipient of the services, meaning the individual that is interacting with you via our services and/or receiving communications from you via our services, referred to as ‘end-user data’ (collectively, “End-User”).

Privacy and protection of personal data is one of our core principles. Our privacy statement is intended to give you a detailed understanding of our data processing practices. It is important to us that the information in this privacy statement is transparent, and you feel well informed and empowered when it comes to the privacy of your and your End-Users’ personal data, as well as the steps we take to protect that personal data.

If you or any of your End-Users are located in Singapore, references in this privacy statement to terms such as "data subject", "data controller", and "data processor" should be taken to refer to the equivalent terms of "individual", "organization", and "data intermediary" under the Personal Data Protection Act of 2012 (“PDPA”).

If you or any of your End-Users reside in California, references in this privacy statement to terms such as “personal data”, "data subject", "data controller", and "data processor" should be taken to

refer to the equivalent terms of “personal information”, "consumer", "business", and "service provider" under the California Consumer Privacy Act of 2018 (as amended by the California Privacy Rights Act) (“CCPA”).

We apply similar data protection standards to all individuals regardless of nationality, geographic location, or data source. As a general principle, personal data is only used when necessary to achieve a purpose, the persons whose data it concerns are properly informed, and there are legal grounds to do so. All activities involving personal data will be checked against the EU’s GDPR or other applicable laws.

1. About our personal data processing practices

We will only process personal data to the extent necessary to fulfill the specific purpose(s) for which you have submitted personal data, unless we are subject to a legal obligation that requires processing of personal data. Section 2.2 of this privacy statement provides you with an overview of the different purposes that may apply to you. Some basic examples of actions that result in us processing your personal data are (a) signing up to our newsletter, (b) signing up for the services via our website and accept the General Terms and Conditions (the “Terms”), or (c) signing up for the services through an order form. To the extent permitted or required by applicable law, you will be given the opportunity to explicitly agree to the collection, use, disclosure, and sharing of the personal data you’ve provided.

When you share personal data with us, we commit to handle that information in accordance with the applicable data protection and e-privacy regulations, including the General Data Protection Regulation (“GDPR”). Due to the nature of the services we do not interact with End-Users directly. You are responsible for ensuring that you have all applicable rights and consents necessary to share any End-User personal data with us, and that the personal data is accurate and complete.

1.1 Roles and responsibilities. When it comes to processing personal data, there are different roles and responsibilities that come into play. For your convenience, this privacy statement provides an explanation of the relevant roles, the corresponding responsibilities of each role, and the systems of governance that play an integral part in protecting your personal data.

The ‘data controller’ determines the purpose (why) and means (how) of personal data processing and remains ultimately responsible for the correct handling of the data subject’s personal data. In practice, the data controller is often the company that an individual (or data subject) provides their personal data to directly.

A ‘data processor’ is a company that provides services to the data controller, and receives personal data from or on behalf of the data controller in order to perform those services. To give an example, when one of our customers sends a marketing campaign through our communications platform, we receive personal data from the customer, such as a phone number or email address of the intended recipient, in order to provide the service. In this example, we act as the data processor of the customer, who in turn is acting as the data controller of the phone number or email address entrusted to it by the individual to which this personal data belongs. The data processor only processes personal data according to the instructions of the data controller, and in line with its own

legal obligations. These instructions are typically laid down in a dedicated data processing agreement between the controller and the processor.

Depending on your relationship with us, we can be either a data controller or data processor, or in certain circumstances we can be both. If you have any questions about these practices or more general inquiries about how we handle personal data, you can contact us at privacy[at]bird.com.

Personal data is collected for specific purposes, including the prevention of spam and fraud, the fulfillment of legal requirements, communication, marketing, sales activities, and ancillary services. Personal information will never be collected, used, or retained without purpose. We do not sell your or your end-users personal data.

2. Why we collect personal data

We have a few key priorities when it comes to protecting your personal data. Not only do we prioritize keeping your personal data safe and secure, we are also committed to protecting your privacy rights and freedoms as an individual. We do not use your personal data for any other purposes than those agreed to by you or as permitted by the Terms and this privacy statement.

2.1 Lawfulness of Processing. All personal data we process will only be processed to the extent we have a legal basis to do so. The legal bases we rely upon for processing personal data are: (a) consent, (b) performance of a contract, (c) compliance with a legal obligation, and (d) legitimate interest.

a) Explicit consent from the data subject. For example, by ticking a box on our website when you want to download product information or submitting a form to be contacted by our sales department.
b) Performance of a contract. This includes not only the provision of the services but also negotiating and signing a contract in order to receive a service.
c) Compliance with legal obligations applicable to us. For instance, preventing misuse of our services, cooperating with formal disclosure requests, and retaining customer account data and financial data.
d) Legitimate interest. This applies (in some jurisdictions) for example to direct marketing activities targeted to existing customers on an opt-out basis. Where we rely on legitimate interest, we have assessed the processing is not high risk, does not involve the processing of special categories of personal data, and will not violate fundamental human privacy rights.

The specific legal basis which permits us to process your personal data may differ when you receive our services from an entity located outside the European Economic Area ("EEA") and as a result the services and our processing obligations may be subject to non-EU data protection requirements.

2.2 Purposes. The purposes for which we process personal information depend on your relationship with us. For starters, you will be required to submit personal data related to you and the business you represent when creating an account. In addition, we may also require personal data in order to enable you and your End-User's (as applicable) to make use of our services. In other circumstances, we may process your personal data to conduct and expand our day-to-day business, for analytical

improvements to the service, support, sales, marketing, to fulfill our statutory legal obligations, and for legitimate business purposes. Personal data can also help us improve the quality of our services and to develop new functionalities to fit the needs of our customers, such as product and experience personalization. In section 3.4 of our Data Processing Agreement (DPA) we refer to these purposes combined as 'legitimate business purposes'.

We only request personal data that is necessary to fulfill the specified purposes listed below as applicable to you; provided, however, if the nature of our relationship with you changes, we may need you to provide additional information or remove personal data that is no longer required. For example, if you fill out a form to request more information about one of our products, we will use your contact information to send the requested product information to you. If you then decide to become a customer, you will need additional information including your billing address for the purpose of account creation and providing you with the services.

The following is a list of purposes for which personal data processing is required. The specific purpose applicable to the processing of your personal data depends on the nature and extent of your relationship with us.

- To share relevant information about our products and services in accordance with your marketing preferences, including important notifications about the services.
- To create an account connected to you and the company you represent.
- To verify your identity.
- To facilitate access and use of the services in line with the Terms.
- For finance and billing purposes, including fulfilling financial obligations such as paying taxes and ensuring invoices are paid.
- To provide customer support and communicate with you about your account and use of the services.
- To analyze usage of our products and services.
- For the transmission of information over the services; defining communications processing priority, routing configurations, and optimizing infrastructure.
- To enforce compliance with the Terms and applicable law.
- To keep our site,your account, and the services safe and secure.
- To detect, prevent, and combat fraudulent or unlawful activity.
- To protect the rights, property, or safety of us, you, our other customers, or any other third party.
- To meet legal obligations, including complying with valid court orders, disclosure requests, subpoenas, and other appropriate legal mechanisms.
- To conduct questionnaires and surveys in order to provide better services to you, our other customers, and End-Users; provided, however your participation in and completion of any questionnaires is always voluntary.
- To apply cookies in line with your cookie consent management settings.

3. What personal data we collect and how

The exact type of personal data we collect depends on the relationship we have with you and the processing purposes that apply to you. . Applying your cookie management settings on our website,

signing up for a newsletter, downloading marketing materials, requesting to be contacted by our sales team, creating an account, or using any of our products and services, are all examples of actions you take that require you to share certain personal data with us that is specific to that particular interaction.

3.1 Personal data directly collected from you. The categories of personal data we collect from you include personal identifiers, employment or professional information, financial information, commercial information, information related to internet activities, and location related information.

- Personal identifiers. When you create an account and make use of any of our products and services, you are required to provide us with personal identifiers. Personal identifiers submitted as part of account creation or use of products and services are referred to as "Customer Account Data". Customer Account Data consists of your name, contact details such as business address, phone number, and email address, financial information, photo (optional), bio description , and signature (subject to our business interactions). Additionally, when you request product related information, to be contacted by our sales team, or attend events, we may request personal identifiers from you such as your name and contact details.

- Employment or professional information. The information we process about you that relates to your employment or profession, the company you work for, and your job title.

- Financial information. The payment and billing information we require you to share with us or directly with a payment-service provider, such as billing name and related address, bank account number, or credit card information.

- Commercial information. Commercial data relates to your interest in products, your use of services, platforms, and account dashboards, and any of our web pages you visit.

- Internet activity information. When you interact with our websites, marketing emails, and services, data is collected about your device and browser, time zone setting, web pages visited, products you view or search for, page response times, download errors, length of visits to certain pages, page interaction information, internet protocol (IP) address used to connect your computer to the internet, use of cookies, pixels, or similar technologies.

- Location related information. The use of our services and products involves the processing of location related information. The type of data involved will differ depending on the service you use but location related information may include your and/or your End User's IP address, business address, and service traffic related metadata such as the routing path and terminating carriers.

- Support interaction information. When you interact with our Customer Support team over phone or email we process the phone number or email address that you use, and the content of your query. In case of a phone call we will inform you that the call may be recorded in accordance with applicable laws.

We only request and retain personal data when strictly necessary. The data that we request will be relevant to our relationship and your purpose. For example, we require an email address to be able to send you marketing emails, but we do not need your gender or payment information.

3.2 Personal data collected from other sources. We collect personal data we obtain from sources other than you ("Third Party Data"). Third Party Data may include, but is not limited to, (a) personal identifiers, and (b) employment or professional information, such as company name, company description and website, company (estimated) revenue and employee range, company industry, employment role and title, seniority, full name, and phone number. The information we collect about you from other sources is business related but even in a business relationship certain information might be considered personal data.

Third Party Data is collected from the following sources:

- Third party service providers of business information. We obtain business data such as employment or professional information from third parties. This information includes email addresses, the company an individual works for, job titles, phone numbers, and URLs of LinkedIn profiles. We obtain this information to expand our business through direct marketing, targeted advertising, and event promotion. Third Party Data may be combined with personal data that you provide to us. Information can be used to develop our business by updating, expanding, and analyzing our customer relationship records.
- Third party social media providers. Depending on your and/or your End Users' privacy settings, third party social media service providers such as Google, Twitter, and Facebook can provide us with information about you or an End User, as applicable. However, if you or an End User connects to a social media page you may (depending on the platform) be presented with the option to decide whether or not you would like to share that information with us. Third Party Data may be combined with personal data that you provide to us. Information can be used to develop our business by updating, expanding, and analyzing our customer relationship records.
- Third party services & connectors. We make connectors available on our platform that will allow our services to be used in connection with third party services through APIs or other connectors. For the sole purpose of enabling and facilitating the connector, your information may be made available to or shared by our services with the relevant third party service (and vice versa). Personal data that we may receive from the third party service provider on your behalf are contact data, activities and event data. Activities and event data may include personal data in case you as a customer include such information in the use case that you apply to the use of the services.
    - **Google API & Connectors:** When you as a customer are making use of a connector service that involves the use and transfer of information received from Google API to any other application, you are required to adhere to Google API Services User Data Policy, including the Limited Use requirements mentioned therein.
- Resellers & Partners. In the event you purchase our services through an authorized reseller, the reseller may exchange information with us, and vice versa, for the sole purpose of the Reseller Sales Agreement and the Terms. In the event you purchase services from us following a referral from an authorized partner or you purchase the consultancy services of third party partners (such as implementation services) in respect of our services, limited information can be shared with us by the partner, and vice versa, solely in connection with the referral and discharging any referral fee payments owed by us to the Partner, or solely to assist you in procuring the third party consultancy services in respect of our services.
- Someone else working for your company. Colleagues of yours can provide us with personal data about you such as your name, job title, email address, or phone number.

If you no longer want to be contacted by our sales and marketing teams, you can always unsubscribe from an email campaign by contacting your account manager or our Support team via support[at]bird.com.

Subject to any exceptions noted in this privacy statement or in the Terms, you will always have a choice when it comes to the types and extent of the personal data you share with us. When we ask you to provide personal data to us, you can decline. However, many of our products and services require personal data so your choice not to provide personal data in certain instances can prevent you from using a certain product, service, or functionality.

End-User personal data per service

Services	**Categories of End-User personal data involved**
SMS	Phone number, traffic data*, location related data**, communication content
Voice	Phone number, traffic data*, location related data**, communication content recordings (optional)
Email	Identification and contact data (name, email address, and other demographic and segment data provided by you as the customer). IT information (IP addresses, usage data, cookies data, online navigation data, location data, browser data). Communication content.
Numbers (local numbers, short codes, Programmable Numbers API)	None. Please take the additional service into account that is used in combination with the Numbers service, such as Voice or SMS to get the correct understanding of personal data involved, as applicable to you.
Inbox	Customer agent data, service/channel specific data
Flow Builder	Email address, phone number, or channel ID contained in Flow Builder invocations created by the customer, service/channel specific data
Video	Meeting information: • Meeting date • Meeting description • Meeting review (optional) • Meeting wrap-up (optional)

	• Audio and/or video recording of the meeting (optional) Guest information: • Guest name • Guest email • IP address • Guest phone (optional)
Omnichannel Widget	Email address, phone number, channel identification, preferred channel of communication, IP address, traffic data*
Conversation Channels (WhatsApp for Business, Google Business Messages, Facebook Messenger, Instagram, Line, Twitter, Viber, WeChat)	Phone number or channel identification, traffic data*, communication content.
Push Notifications (Push RTC Channels Service and Push Beams Service)	IP address, traffic data*, communication content.
CDP	Name, email address, job title, IP address
* Traffic data is data that is processed for the purpose of transmitting communications, such as routing data, and data about the date, time, and duration of the communication. ** Location related data is data with which the geographical position of the carrier or the communication equipment can be determined on the basis of the supplier used.	

Personal data is only shared with third parties when necessary or when legally required. Data can be shared with government authorities and affiliated businesses, including communications and technology service providers. Third parties must meet strict privacy and security practices.

4. Parties we share personal data with

We share personal data with third parties but only in limited instances. Regardless of whether we fulfill the role of data controller or data processor, when we share personal data with third parties we always make sure that the third parties we share any personal data with adhere to similar data protection and security standards as outlined in this privacy statement and the data processing agreement. There are seven categories of third parties with which we may share personal data:

1. (Tele)Communications services providers
2. Third party service and technology providers
3. Payment service providers (PSPs)
4. Our Partners
5. Our Affiliates

6. Government authorities, when required to do so by law

4.1 (Tele)Communications Services Providers. To provide you with certain products and services, we engage with telecom operators, aggregators, carriers, and other communications service providers for routing and connectivity purposes. In order to make sure the message you sent will reach the intended recipient regardless of their physical location, we use a global network of telecom providers. When it comes to the contents of electronic communications transmitted by communication providers, these operators, aggregators, and service providers are neither data controllers nor data processors because they act as mere conduits for the transmission of communication content. If communications services providers process any personal data for their own purposes (e.g. fraud prevention, billing, filtering, or legally required data retention activities) they act as data controllers.

4.2 Third party service and technology providers. We share personal data with third party service providers, like analytics, data science, and fraud prevention service providers, cloud hosting providers, and third parties used to set up the connectors that a customer wants to make use of. We never share information with a third party without vetting them in advance and having the required contractual, technical, and organizational safeguards in place. An overview of third party service providers that process personal data can be found via the section 'Approved Processors' of this privacy statement.

4.3 Payment Service Providers (PSPs). When you pay for our products and services, PSPs provide you with two ancillary services in addition to the basic provision of payment services: (a) Saved Payment Methods and (b) Auto Recharge. Stripe, Mollie, and Adyen are the PSPs that collect, process, and store all of your payment requests and do so as data controllers in their own right.

- Saved Payment Methods functionality allows customers to save financial information for a specific payment method on a consent basis for convenience reasons. The information necessary to provide this service differs depending on the selected payment method (for example, credit card, iDeal, or Paypal). For a credit card, you are required to provide the last four digits of a credit card number, the expiration date, and the name of the cardholder. For iDeal, you are required to provide the IBAN/BIC number and account name. For PayPal the only required information is your PayPal account email address.
- Auto Recharge functionality allows you to automatically top up your account balance if it falls below a minimum threshold predetermined by you. You can enable this ancillary service through a toggle button, by which you provide your consent for us and our PSPs to use your payment information to automatically recharge the credits on your balance. Your preferred bank may request extra authentication from you before you can use the Auto Recharge functionality.

For both of these ancillary payment functionalities you can withdraw your consent at any time on the customer finance settings page.

4.4 Our Partners. In the event you purchase our services through an authorized partner (" Reseller"), the Reseller may exchange information with us, and vice versa, for the sole purpose of the Reseller Sales Agreement and the Terms, and you consent to such information exchange. In the event you purchase services from us following a referral from an authorized partner or you purchase the consultancy services of third party partners (such as implementation services) in respect of our services (" Partner"), limited information can be shared with us, and vice versa, solely in connection

with the referral and discharging any referral fee payments owed by us to the Partner, or solely to assist you in procuring the third party consultancy services in respect of our services.

4.5 Our Affiliates. In order to do business globally, we might need to share personal data between our Affiliates. This can apply to customer support assistance, international sales activities, or in order to facilitate the provision of the services. Both we and our Affiliates will only use personal data as described in this privacy statement, the Terms, the DPA, and only to the extent permitted under applicable law.

4.6 Government Authorities. We will not share your information with third parties outside of those outlined in this privacy statement or without your permission, except when we're legally required to do so and in accordance with our Disclosure Requests Policy. We will provide you with a notice in case a governmental authority requests information from us about you or your customers, unless this is explicitly forbidden by law. If authorities do not want us to notify our customers, we require them to explicitly reference the legal grounds that would prevent us from doing so in the disclosure request. We push back on any disclosure request to the extent we have a reasonable legal basis to do so. The Disclosure Request Policy addresses circumstances in which we are legally obligated to respond to official government requests for disclosure of information, and the requirements for government requests to be processed in accordance with our policy and law.

Sometimes, we need to transfer personal data to business partners located outside of the European Union. We have robust privacy procedures in place that we deploy as required to protect the privacy of individuals both inside and outside the EU.

5. International transfer of personal data

As a global cloud based service provider, the use of our services often involves the transfer of personal data to recipients and third parties both inside and outside the European Economic Area ("EEA"). We are also an international employer, providing its workforce with the ability to work from different geographical regions. A practical example is that we apply 'follow the sun support' to our customer support practices, allowing for ongoing and continuous support regardless of the time or location. We take care to ensure our partners regardless of location have sufficient safeguards in place to properly process and protect your personal data in line with our own data protection and information security standards.

One of the important steps we take when it comes to international data transfers involving third parties is due diligence and vetting. As part of the third party vetting process, we ensure that personal data will only be transferred to a third party located outside the EEA with the required cross-border transfer mechanism and safeguards in place. This means that when we engage a third party that is located outside of the EEA, we agree on the appropriate level of data protection, including additional contractual, technical, and organizational measures and the execution of a transfer impact assessment where necessary, to ensure the ongoing protection of the rights and freedoms of all individuals, inside and outside the EU. We consistently monitor changes to the international transfer mechanisms permitted under applicable privacy laws to ensure ongoing compliance with the international data protection standards.

The Data Privacy Framework & MessageBird USA Inc.

MessageBird USA Inc ("**MessageBird USA**") complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF), (together "DPF"), as set forth by the U.S. Department of Commerce. MessageBird USA has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union and the United Kingdom in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF. MessageBird USA has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) Program, and to view our certification, please visit https://www.dataprivacyframework.gov/.

MessageBird USA complies with the DPF Principles for all onward transfers of personal data originating from the EU, UK, and Switzerland, including the onward transfer liability provisions. MessageBird USA is responsible for the processing of personal data it receives under the DPF and subsequently transfers to a service provider acting as a (sub)processor or agent on its behalf. MessageBird USA requires third parties and service providers to which it discloses personal data to protect personal data using substantially similar standards to those required by MessageBird USA and at least the same level of privacy protection as is required by the DPF and this Privacy Statement. MessageBird USA shall remain liable under the DPF Principles if its service provider(s) processes such personal data in a manner inconsistent with the DPF Principles, unless the organization proves that it is not responsible for the event giving rise to the damage.

With respect to personal data received or transferred pursuant to the DPF, MessageBird USA is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, MessageBird USA commits to resolve DPF Principles-related complaints about our collection and use of your personal information. EU and UK individuals and Swiss individuals with inquiries or complaints regarding our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF should first contact MessageBird USA at: privacy[at]bird.com.

Where applicable, MessageBird USA offers individuals whose personal data is processed in reliance on the DPF the opportunity to choose (i.e., opt out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals, unless processing by the third party is done as an agent (in which case MessageBird USA will enter into a contract with the third party agent), or is required due to a statutory legal obligation that applies to MessageBird USA. Individuals can exercise choice and right, in line with the DPF choice principle, by reaching out to privacy[at]bird.com as well.

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, MessageBird USA commits to refer unresolved complaints concerning our handling of personal

data received in reliance on the EU-U.S. DPF, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. DPF to the Data Protection Authority that is relevant for you. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit the website of the EU/EEA Member State data protection authority; UK Information Commissioner's Office (ICO) or Gibraltar Regulatory Authority (GRA); or the Swiss Federal Data Protection and Information Commissioner for more information or to file a complaint. The services of the DPAs are provided at no cost to you.

Under certain conditions, more fully described on the Data Privacy Framework website available here, you may be entitled to invoke binding arbitration after other dispute resolution procedures have been exhausted. Additional information is available here for EU/EEA and UK (and Gibraltar) individuals and here for Swiss individuals.

Proper security measures are required for effective data protection. Our measures have been created with the highest standards of confidentiality in mind. We hold several information security certifications, including ISO27001 and SOC 2.

6. The data protection and security standards we apply

Data security is paramount to us. To minimize security risks, we invest in state-of-the-art technology, thorough security screenings of our infrastructure and employees, and employ industry standard security measures. Additionally, depending on the platform, services, and products you are using, we hold multiple globally recognised information security standards for Information Security Management Systems, like ISO27001 and SOC 2 Type II compliance. All of our hosting providers are ISO27001 and SOC 2 Type II compliant as well.

Since all our accounts to access our platform services are password protected (with optional two-factor authentication), you should be the only person with access to your account. You are responsible for safeguarding the credentials to your account. If your login information is stolen or used without your permission, it is imperative that you notify us immediately so we can take steps to secure your account. You can notify us of any unauthorized use of your account by sending an email to security[at].com with the subject 'Urgent: account credentials'.

If you want to know more about the measures we take to keep your data secure, please take a look at our public Security Overview and the Technical and Organizational Security Measures. These web pages contain information about the industry standard, administrative, technical, physical, and organizational safeguards designed to prevent unauthorized access and use of your personal data.

The length of time that we retain personal data for is determined by a combination of legal requirements, instructions from customers, and the duration of time necessary to achieve the purposes for which the information was collected.

7. How long we retain personal data

The duration for which we are required or allowed to retain personal data depends on the nature and the purposes for which the personal data is processed. We retain personal data only to fulfill

contractual or legal obligations applicable to us or the specific Affiliate you contract with (as outlined in the Terms). The applicable legal retention requirements for personal data retention may vary depending on the geographical location of us or the Affiliate you are contracting with, or where the communications services are being terminated.

7.1 SMS and Voice services. Personal data related to the use of SMS and Voice services have a default retention period of six (6) months. The retention of personal data related to those services are necessary (a) to fulfill our legal obligations to ensure the integrity and security of our services, and prevent misuse of telecommunications services, (b) for the transmission of information over the services, and (c) to ensure we are able to fulfill our legal obligations to assist formal governmental authorities. For more information on disclosure requests please review our Disclosure Request Policy. In other jurisdictions, retention obligations for telecommunication service providers can be for an extended period of time and may be up to two years.

7.2 Email services

The email services consist of three product categories; design, delivery, and deliverability. Design products do not require processing of personal data. They do not facilitate the sending of emails. The delivery products, such as Email Cloud sending do require personal data to be processed; i.e. recipient email address. Such personal data is retained for a brief period of 10 days, after which the data is protected by means of a one-way hash. A backup of a message event is retained for 30 days and then automatically deleted. We do not store the message body (i.e., the content of the email) after it has either been delivered or bounced. A delivery or bounce typically happens within seconds. However, a message can stay on the retry queue for up to 72 hours between the time it is injected and the time it bounces. On premises delivery products do not require the processing of personal data by us. The Deliverability products Inbox Tracker and Competitive Tracker do not require processing of personal data either.

7.3 Omnichannel communication services. For all other communications services, features, and products personal data is retained for the duration of our contract with you, our provision of the services to you, or where possible for a different period as agreed upon with you as the customer. In addition, we provide certain ancillary services which include, but are not limited to, the ability to maintain an online address book 'Contacts' for your convenience, and insights into account specific communication usage and transmission history. The personal data related to those ancillary services will be retained for the duration of our contract with you or our provision of the services to you. You acknowledge and agree that any end-user/communication recipient personal data, such as phone numbers, email addresses, etc, are controlled by you and any data protection rights exercised by your End Users must be actioned by you. It is your responsibility as a data controller or acting on behalf of a data controller to ensure compliance with your obligations towards End Users whose personal data you control.

7.4 Marketing and Sales. We keep personal data for marketing and sales purposes up to twelve (12) months, or, if you are an existing customer, for the duration of the services, unless you have withdrawn your consent or unsubscribed from receiving marketing information.

7.5 Compliance with corporate and financial legal obligations. We are under an obligation to demonstrate compliance with applicable national, union and federal financial and tax laws and regulations. As a telecommunications service provider, we are required to retain customer data such

as name, email address, (company) address, (company) bank details, invoices, services used, and role of the customer's representative for a period up to ten (10) years.

Proof that consent has been given or has been withdrawn for the processing of personal data, where applicable, will be retained for five (5) years.

After a retention period expires, we may keep personal data in a non-identifiable form for archival, statistical, and/or other legitimate business purposes. None of the data will be able to identify an individual directly or indirectly.

Please note that we are not always in a position to fulfill a personal data erasure request if the request conflicts with one of our legal retention obligations. Since we are required to demonstrate that legitimate exercise of rights requests have been fulfilled, we retain confirmation emails relating to these requests for five (5) years.

We have measures in place to allow you to exercise your data protection rights, including having your data erased. In some situations, our statutory legal obligations may prevent us from fulfilling data privacy requests.

8. How to control your data protection rights and choices

Even though we collect your personal data for the various purposes outlined in this privacy statement, your personal data stays your own. You are in control of your personal data, as well as the personal data of End Users you provide to us as a customer (if applicable). Unless we are under a legal obligation, your data protection rights and freedoms are controlled by you.

You can change your cookie management settings as a website visitor, withdraw consent to our processing of your data if applicable, control and review your personal data, object to the processing of personal data when this is done on the legal basis of legitimate interest, or obtain restriction of the processing of data if necessary in accordance with applicable data protection laws.

Where we need to collect personal data by law, or under the terms of a contract we have with you, and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with services). In this case, we may have to cancel a product or service you have with us but we will notify you if this is the case at the time.

8.1 Exercising your data protection rights: control your personal data.

If you have an account for any of our products or services at our connectivity, email, or engagement platforms you can view, amend, delete, and transfer the personal data you control (including the personal data of your End Users). If you want to exercise control over your or your End Users' personal data, you can do so via the privacy dashboard on your online account. We provide all of our customers with reasonable assistance to fulfill their obligations as a data controller towards the recipients of the communications you have sent over our platform. In order to verify your identity, or the validity of a request you make on behalf of the end-user whose data you control, we have made technical and organizational measures available that allow you to fulfill these obligations via your

online account. For the avoidance of doubt, you as a customer acting as a data controller are responsible for processing any requests or complaints on behalf of your End Users whose personal data you control.

If you do not have an account for any of our products or services, and therefore do not have access to the privacy dashboard you can exercise your personal data rights by sending a request to privacy[at]bird.com.

8.2 Withdraw consent to our processing of your personal data. If you have provided us with your personal data on a consent basis and you no longer want us to use that personal data for any reason then you are always free to change your mind and revoke consent. If you make a legitimate withdrawal of consent request to us, we will always comply with your request, unless we're legally required to keep your personal data (such as to demonstrate that we have acted upon a withdrawal of consent request).

8.3 Object to and restrict the processing of data. If we are processing your personal data using a legitimate interest basis, you have the ability to object to this processing and can exercise your right to restrict this processing. If you exercise your right to restrict personal data we process on a legitimate interest basis, we will assess each request on a case-by-case basis according to the rules set out by the applicable data protection laws. If we reject your request we will demonstrate that we have compelling grounds to do so or that there's a legal claim which allows us to retain personal data. If you do not agree with how we've handled your request, you can file a complaint with the data protection authority of The Netherlands, the authority related to the European member state you live or work in, or the country in which the suspected infringement of your right to restrict personal data has taken place. We would, however, appreciate the chance to address your concerns before you approach the applicable data protection authority, so please contact us in the first instance.

8.4 Processing time of data subject requests. Under normal circumstances, we will process your request as soon as possible but no later than within one (1) month of receiving the request. If a request is complicated or we receive too many requests during a given time period, our response time may be extended up to two (2) months from the date the request was received. We will inform you if you should expect a two (2) month response time. When you choose to delete your personal data, we may hold onto fully anonymised and aggregated data. If we do so, this anonymised and aggregated data will not be able to identify you as a person in any way. If we're required to retain your information for legal reasons, we will let you know when we respond to your request. Specifically for California based individuals, consumers shall not be discriminated against because of the exercise of their rights under the CCPA.

When you use one of our websites we will ask you to confirm your cookie preferences. Depending on your choice, this allows us to place cookies or similar technologies on your device. A cookie is a small text file saved on your device that collects information about your interactions on our web pages.

9. Cookie notice

When you use our website, we place small data files, called cookies, or similar technologies on your browser. A cookie is a small text file saved on your computer or mobile device when you visit a website.

In the cookie manager reference is made to the privacy statement. In this cookie notice we will explain in clear and plain language the relevant details about our use of cookies, including where cookies are hosted, the lifespan of cookies, and the purpose of cookies. This list is subject to change and it may not include all cookie providers at any given time. Website visitors are enabled to select the cookie categories they would like to apply to their device by means of the cookie consent management, and by doing so active consent is given.

Cookies are divided into three categories: mandatory cookies that do not involve personal data and are strictly necessary for the operation of our web pages, opt-out cookies that do not involve personal data and are helpful for our analytics, and opt-in cookies which do involve the processing of personal data and we use for marketing and advertising purposes.

9.1 Types of cookie categories. Our websites primarily use four types of cookies; *Strictly necessary, Analytics, Functional, and Advertising* cookies. These include first and third party cookies: first party cookies are set and controlled by us, while third party cookies are set and controlled by a third party tool or service provider. The duration for which a cookie is set varies. Session cookies disappear from your computer or browser when you logout of your account or close your browser, while persistent cookies are stored even after you have closed the page. The retention periods for cookies are specified below. With the exception of strictly necessary cookies, cookies will only be placed on your device and/or browser after you confirm or update your preferences through the cookie management settings.

If you decide to not allow opt-in performance and functional cookies on a site, the site may not function fully as designed. For example, you may face issues logging in or retaining set preferences, such as the preferred language the website displays.

- **Strictly Necessary.** These cookies are necessary for the website to function and cannot be switched off in our systems. They are set in response to actions made by you which amount to a request for services, such as setting your privacy preferences, logging in, or filling in forms.
- **Functional.** These cookies enable the website to provide enhanced functionality and personalisation such as the website content being provided in the preferred language for your location. They may be set by us or by third party providers whose services we have added to our pages.
- **Performance.** These cookies allow us to measure visits, traffic sources, and engagement so we can improve the performance of our site. They help us learn which pages are the most and least popular and see how visitors move around the site. All information these cookies collect is aggregated and therefore anonymous.
- **Marketing.** These cookies allow advertising parties to uniquely identify your browser and internet device. These cookies have the capability to either alone or in conjunction with others uniquely identify a person directly or indirectly. They may be regarded as personal data under the relevant Data Protection Legislation.

Unclassified cookies are cookies that we are in the process of classifying, together with the providers of individual cookies.

IP Addresses: when you visit our website or account portal or use our products and services, we process your IP address. We use IP addresses to track and analyze information about the devices that interact with our systems and to know where these devices are located. For example, for the purpose of detecting the location of customer account logins to help us combat potential fraud or malicious activity.

Web Beacons: a web beacon is an object placed in a web page or email we use to check whether a user has accessed its content. We use web beacons along with cookies to gather data about your use of our site and account portal. For example, we may use web beacons in marketing emails that notify us when you open an email or click on a link.

9.2 Change your cookie settings. When you visit one of our websites for the first time, you can either allow us to place all the cookies we use on your browser, decide to accept specific cookies, or deny all cookies that are not strictly necessary. You can always change your preferences either in your browser settings or in the cookie settings on our website. Within our cookie management settings, we outline each cookie type in use on our site and provide an explanation of the implications of accepting each cookie type.

9.3 Manage cookies from your browser. Find out more on how to update, activate, deactivate, or remove cookies using your browser by visiting the links below:
Google Chrome
Firefox
Safari

Global Privacy Control. Global Privacy Control (GPC) is a technical specification that you can use to inform websites of your privacy preferences in regard to ad trackers. To set up GPC, you can visit the Global Privacy Control page. Please note that this may impact the functionality of our websites or your account.

Do-Not-Track. Currently, our systems do not recognize browser "do-not-track" requests. You may, however, disable certain tracking as discussed in this section (e.g., by disabling cookies).

10. Children

Our services and products are not directed to or intended for children under the age of 18. We never knowingly collect and/or process any personal data from children below the age of 18. If we discover that we have received personal data from a child without parental or legal consent, we will take reasonable steps to delete that information as quickly as possible. If you believe we have any information from or about a child, please contact us at privacy[at]bird.com with the subject: 'Children'.

11. Links, third party websites and social networking sites

Our online services and communications may embed hyperlinks to websites that are not owned or controlled by us. We are not responsible for the privacy practices, policies, notices, or content that are not owned or controlled by us. We encourage you to read and understand the privacy practices, policies, notices, and content of any linked sites that you visit.

12. Changes to our privacy statement

This privacy statement is subject to change. We reserve the right to change, update, modify, or remove any part of this privacy statement at any time. If any modifications substantially affect your rights under this privacy statement, we will notify you where possible. You can always decide to discontinue your use of our services if you disagree with any updates we may make to this privacy statement.

13. Disputes

If you have any dispute with us relating to our privacy practices, please contact our legal team at privacy[at]bird.com with the subject: 'Dispute'. If we are unable to reach an understanding via email, please refer to the Terms, which describes how disputes will be resolved between us. Please be sure to review the Terms before you use any of our products and services.

14. Approved Subprocessors

An overview of the third-parties used for the processing of personal data can be found here. In addition, the Help Center page contains a 'subscribe' button that allows you to subscribe to notifications of changes to our use of third-party (sub)processors.

15. How to contact us

If you have any questions left regarding the processing of personal data after reading this privacy statement, or when you have feedback or suggestions to make this privacy statement better, please do not hesitate to contact us.

If you're not satisfied with our reply, you may refer your complaint to the relevant regulator in your jurisdiction.

If you're not satisfied with our reply, you may refer your complaint to the relevant regulator. You can reach our Data Protection Officer, at privacy[at]bird.com.