PRIVACY POLICY

We know that you care how information about you is used and shared, and we appreciate your trust that we will do so carefully and sensibly. By visiting our website, you are accepting the practices described in this Privacy Policy. In this Privacy Policy, "we", "us" and "our" refer to RegNest, Inc.

What Personal Information About Customers Do We Gather?

Information You Give Us: We receive and store any information you enter on our website or give us in any other way. We use the information that you provide for such purposes as responding to your requests, providing our services (e.g., domain name registration, DNS hosting, etc.), and communicating with you.

We receive and store certain types of information whenever you interact with us. For example, like many websites, we use "cookies," and we obtain certain types of information when your browser accesses our sites. Examples of the information we collect and analyze include the Internet protocol (IP) address used to connect your computer to the Internet; computer and connection information such as browser type and version, operating system, and platform; and the full Uniform. Resource Locators (URL) click stream to, through, and from our website, including date and time. We use IP addresses to analyze trends, administer the site, track user movement, and gather broad demographic information for aggregate use.

What About Cookies?

Cookies are alphanumeric identifiers that we transfer to your computer's hard drive through your browser to enable our systems to recognize your browser. Besides using the information as described above, we utilize cookies to control the flow of the ordering processes by maintaining the state of your online transactions. Some of our business partners (e.g., advertisers) may use cookies on our website; however, we have no access to or control over these cookies.

Do We Share the Information We Receive?

Yes, we do share information we receive but only as described below. Otherwise we will not provide your personal information without your consent. We may be subject to liability in cases of onward transfer to third parties that do not conform with this Privacy Policy.

WHOIS: We are required by the Internet Corporation for Assigned Names and Numbers ("ICANN"), the organization that assumes responsibility for domain name allocation, to collect information about you during the domain name registration process. This information includes your full name, mailing address, phone number, email address, and, where provided, your facsimile number. ICANN then requires us to make your full name, mailing address, phone number, email address, and, where provided, your facsimile number, as well as the creation and expiration dates

of your domain name registration and the name server information associated with your domain name (WHOIS Information), available to the public via an interactive webpage and a "port 43" WHOIS service, unless you utilize a proxy service approved by us. In the event you elect to utilize a proxy service approved by us, the information of that proxy service, rather than your WHOIS Information, will be made available to the public. Please note that we are not able to control how members of the public may use the WHOIS Information.

Affiliates: We are a member of the RegNest Inc. The Family of Companies includes the following websites: Regnest.com, Regnest.ge. The Family of Companies also includes the following non-U.S. based companies: RegNest LLC (Georgia). We may share information we have about you within the Family of Companies to facilitate, support, and integrate their activities and improve our services. Each U.S. based member of the Family of Companies adheres to the Privacy Shield Principles (as discussed below).

Advertisers: We will share aggregated demographic information with our partners and advertisers. This is not linked to any personal information that can identify any individual person.

Partners: We partner with other parties to provide specific services. When the user signs up for these services, we will share names, or other contact information that is necessary for the third party to provide these services.

Agents: We engage other companies and individuals to perform functions on our behalf. Examples include processing credit card payments, providing marketing assistance, providing customer services, sending postal mail and email to you, removing repetitive information from customer lists, and analyzing data. These persons have access to personal information needed to perform their functions. These companies do not retain, share, store or use personally identifiable information that you provide to us for any secondary purposes.

Service Providers: We engage other companies and individuals to perform enhanced services on our behalf. In addition, certain of our enhanced services require that we contact Internet directories and various search engines on your behalf. Many of our service providers have access to personal information needed to perform their services. These parties are not allowed to use personally identifiable information except for the purpose of providing these services.

Business Transfer: As we continue to develop our business, we might sell or buy businesses or their assets. In such transactions, customer information generally is one of the transferred business assets. Also, if we or all or substantially all of our assets were ever to be acquired, customer information will of course be one of the transferred assets.

Compliance: We release account and other personal information when we believe release is appropriate in response to a lawful request by public authorities, including to meet national security or law enforcement requirements; enforce or apply our agreements; or protect our rights, property, or safety, our users, or others. This includes exchanging information with other companies and organizations for fraud protection and credit risk reduction.

How Secure Is Information About Me?

We work to protect the security of your information during transmission by using Secure Sockets Layer (SSL) software, which encrypts information you input and the information we may send to our agents.

We have gone to great lengths to ensure your information is securely obtained and held in compliance with the Payment Card Industry Data Security Standard. For example, we encrypt your credit card number before it is stored in our database. This helps ensure that no one may access your credit card from our system.

It is important for you to protect against unauthorized access to your password and to your computer. Be sure to sign off when finished using a shared computer.

What Information Can I Access?

We give you access to certain information about you for the limited purpose of viewing and, in certain cases, updating that information. To view or change this information, log in to your account. When you update information, we usually keep a copy of the prior version for our records.

Links

Sites provided by us contain links to other sites. Please be aware that we are not responsible for the privacy practices of such other sites. We encourage our users to be aware when they leave our site and to read the privacy statements of each and every website that collects personally identifiable information.

This privacy statement applies solely to information collected by this website.

Children

We do not sell services for purchase by children. If you are under 18, you may use our services only with involvement of a parent or guardian.

For European Union Citizens or Swiss Citizens

Privacy Shield Frameworks

RegNest Inc., complies with the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries and Switzerland. We have certified that we adhere to the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse,

Enforcement and Liability. If there is any conflict between the policies in this Policy and the

Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit https://www.privacyshield.gov/

Note that you have the right to access, correct, or delete your personal data processed by us. For assistance with accessing, correcting, or deleting your personal data, please contact us at info@regnest.com. Please be aware that deleting your personal data may result in termination of the services you receive through us.

In compliance with the Privacy Shield Principles and GDPR, We commit to resolve complaints about your privacy and our collection or use of your personal information.

REGNEST

General Data Protection Regulation (GDPR)

A guide to the European privacy and data protection changes

An overview of the new privacy and data protection laws that enter into effect on May 25, 2018, and a few best practices towards GDPR compliance

The GDPR is the most important change in data privacy regulation in decades. Companies are working to implement sweeping changes to their systems and contracts, and those running on compliant and privacy-conscious platforms have a head start. This guide aims to help our users understand the GDPR's widespread consequences, the opportunity it affords to improve data processing activities, and how to become and remain GDPR-compliant.

The fine print: This GDPR Guide is for informational purposes only. It is not legal advice. Please reach out to your legal counsel to receive tailored guidance on how the GDPR may affect your business.

What is GDPR?

The General Data Protection Regulation ("GDPR") is a new, EU-wide privacy and data protection law. It calls for privacy that is more guardrails that are granular in an organization's systems, more nuanced data protection agreements, and more consumer-friendly and detailed disclosures about an organization's privacy and data protection practices.

The GDPR replaces the EU's current data protection legal framework from 1995 (commonly known as the "Data Protection Directive"). The Data Protection Directive required transposition into EU Member national law, which led to a fragmented landscape of EU data protection law. The GDPR is an EU regulation that has direct legal effect in all EU Member States, i.e., it does not need to be transposed into an EU Member States' national law in order to become binding. This will enhance consistency and harmonious application of the law in the EU.

The GDPR can apply to organizations located outside the EU

Unlike the Data Protection Directive, the GDPR is relevant to any globally operating company, not just those located in the EU. Under the GDPR, organizations may be in scope if (i) the organization is established in the EU, or (ii) the organization is not established in the EU but the data processing activities are with regard to EU individuals and relate to the offering of goods and services to them or the monitoring of their behavior.

Processing personal data is a broad concept under the GDPR

The GDPR governs how organizations processes personal data of EU individuals. “Personal data” and “processing” are frequently used terms in the legislation, and understanding their particular meanings under the GDPR illuminates the true reach of this law:

Personal data is any information relating to an identified or identifiable individual. This is a very broad concept because it includes any information that could be used on its own, or in combination with other pieces of information, to identify a person. Personal data is not just a person’s name or email address. It can also encompass information such as financial information or even, in some cases, an IP address. Moreover, certain categories of personal data are given a higher level of data protection because of their sensitive nature. These categories of data are information about an individual’s racial and ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, genetic data, biometric data, health data, information about person’s sex life or sexual orientation, and criminal record information.

Processing of personal data is the key activity that triggers obligations under the GDPR. Processing means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not 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. In practical terms, this means any process that stores or consults personal data is considered processing.

Key concepts: data controllers and data processors

In EU data protection law, there are two types of entities that can process personal data — the data controller and the data processor.

The data controller (“controller”) is the entity which, alone or jointly with others, determines the purposes and means of the processing of personal data. The data processor (“processor”) is the entity which processes personal data on behalf of the controller.

It is important to determine whether the entity processing personal data for each data processing activity is a controller or a processor. This mapping exercise enables an organization to understand what rights and obligations attach to each of its data processing operations.

RegNest Inc has certain data processing activities for which it acts as a data controller, and others for which it acts as a data processor. A good illustration of this dual role is when RegNest Inc processes credit card transactions. Facilitating a transaction requires the processing of personal data, such as the cardholder’s name, credit card number, the credit card expiry date, and CVC code. The cardholder’s data is sent from the RegNest Inc user to RegNest Inc via the RegNest Inc API (or by some other integration method, such as RegNest Inc Elements). RegNest Inc then uses the data to complete the transaction within the systems of the credit card networks, which is a function that RegNest Inc performs as a data processor. However, RegNest Inc also uses the data

to comply with its regulatory obligations (such as Know Your Customer ("KYC") and Anti Money Laundering ("AML"), and in this role RegNest Inc is a data controller.

Legal basis for processing personal data in the GDPR

The next consideration is to determine whether or not a particular processing activity is GDPR-compliant. Under the GDPR, every data processing activity, performed as a controller or processor, needs to rely on a legal basis. The GDPR recognizes a total of six legal bases for processing EU individuals' personal data (in the GDPR, EU individuals are referred to as "data subjects"). Those six legal bases, in the order of Art. 6 (1) (a) to (f) GDPR, are:

The data subject has given

CONSENT

to the processing of his or her personal data for one or more specific purposes;

The processing is

NECESSARY FOR THE PERFORMANCE OF A CONTRACT

to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;

The processing is necessary for the

COMPLIANCE WITH A LEGAL OBLIGATION

to which the controller is subject;

The processing is necessary to

PROTECT A VITAL INTEREST

of the data subject;

The data processing is necessary for the performance of a task carried out in the

PUBLIC INTEREST

or in the

EXERCISE OF OFFICIAL AUTHORITY

; or

The processing is necessary for the

LEGITIMATE INTERESTS

pursued by the entity, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require personal data protection.

There are similarities between the GDPR permitted processing list and the list contained in the Data Protection Directive. However, there are also significant divergences.

The most frequently discussed change made by the GDPR, when compared to the Data Protection Directive, is the tightening of the consent requirements (item 1 in the above list). The GDPR consent requirements include elements such as (i) the requirement that consent be verifiable, (ii) the request for consent must be clearly distinguishable from other matters, and (iii) the data subjects must be informed of their right to withdraw consent. It is also important to be mindful that an even higher consent requirement ("explicit consent") is imposed with respect to the processing of sensitive data.

Another important item to highlight is the legitimate interest item (item 6 in the above list). When relying on "legitimate interest" as supporting the processing of personal data, an organization needs to be aware of the balancing test requirement associated with this legal basis. To satisfy the Accountability Principle under the GDPR, an organization must document its compliance with the balancing test, which includes its approach and the arguments that it considered prior to it concluding that the balancing test was satisfied.

Individuals' rights under the GDPR

Under the Data Protection Directive, individuals were guaranteed certain basic rights with regard to their personal data. Individuals' rights continue to apply under the GDPR, subject to some clarifying amendments. The below chart compares individuals' rights under the GDPR.

DATA SUBJECT ACCESS REQUEST
Individuals have the right to know whether their personal data are being processed, what and how personal data about them is being processed, and what the data processing operations are. The extent of this right has been expanded under the GDPR. For example, when making an access request, individuals must receive additional information, including information about their additional data protection rights under the GDPR that did not exist before, such as the right to data portability.

RIGHT TO OBJECT
An individual may prohibit certain data processing operations where he or she has compelling legitimate grounds. Individuals may also object to the processing of their personal data for direct marketing purposes. The GDPR has broadened the scope of this right in comparison to the Data Protection Directive.

RIGHT TO RECTIFICATION OR ERASURE
Individuals may request that incomplete data be completed or that incorrect data be corrected to

ensure that the processing of personal data be in compliance with applicable data protection principles. The GDPR position is materially the same as the Data Protection Directive, but some procedural protections are increased under the GDPR.

RIGHT TO RESTRICTION
No right to restrict processing. However, the Data Protection Directive provides individuals the right to request the blocking of their personal data where the processing operations are not in compliance with data protection principles, for example when data are incomplete or inaccurate. The GDPR offers individuals the right to request the restriction of the processing of their personal data in certain circumstances, including where the individual contests the accuracy of the data.

RIGHT TO ERASURE ("RIGHT TO BE FORGOTTEN")
Individuals have the right to seek erasure of their personal data if the processing operations were not in compliance with data protection principles. Therefore, this right is very narrow. The GDPR has expanded this right substantially. For example, the right to erasure can be exercised when personal data is no longer necessary in relation to the purposes for which it was collected, or the individual withdraws consent to the processing and no other legal basis supports continued processing.

RIGHT TO DATA PORTABILITY
The Data Protection Directive does not explicitly mention "data portability" as a right of a data subject. EU Member State laws may have implemented additional rights akin to a right for data portability on a national level. Individuals may request that personal data held by one data controller be provided to themselves or another controller.

International data transfers

The topic of international data flows has been a hot topic in recent years, and there has been considerable debate and law reform in this area. It is also close to certain that the laws around international data flows will continue to evolve in the coming years. Today under EU data protection law, certain requirements need to be satisfied before EU individuals' personal data may be transferred outside the EU, unless the organization receiving the personal data is located in a whitelisted jurisdiction (see here for whitelisted jurisdictions).

Under the GDPR, international data transfers are a challenging topic to manage because the law keeps evolving and there are only a handful of data transfer mechanisms available. While challenging, organizations need to keep current with the developments because the compliant flow of personal data is the backbone of any technology company.

One particularly important mechanism for personal data flows from the EU to the United States is the Privacy Shield framework. The EU-US and Swiss-US Privacy Shield is a method of ensuring that an organization offers an adequate level of data protection, by requiring that an organization certify and register according to the requirements of the Privacy Shield framework. RegNest Inc

has certified to the EU-US and Swiss-US Privacy Shield for this reason. RegNest Inc's Privacy Shield certification is here, and our Privacy Shield Policy here. For more information, please visit RegNest Inc's EU data transfers support page here.

More generally, RegNest Inc has international data transfer compliance measures in place governing all of RegNest Inc's global entities' processing of the personal data of EU individuals. These measures are based on the EU Standard Contractual Clauses.

As noted above, international data flows continue to be an area of potential future law reform. For this reason, we are following the legal developments around international data transfer compliance measures very closely, and take every measure available to us to ensure a compliant international transfer of EU data subjects' personal data. This also means that we have built redundancies into our data transfer compliance program to the fullest extent possible and are looking to expand these with the tools available to RegNest Inc under the GDPR.

Non-compliance

The most referenced consequence of non-compliance with the GDPR is the maximum fine that can be levied against a non-compliant organization. The maximum fine that may be levied is 4% of global revenue or 20 million EUR, whichever is higher. Certain other types of infringements carry a maximum fine of 2% of global revenue, or 10 million EUR, whichever is higher.

Less frequently referenced are the data protection authorities' ("DPAs' ") powers under Art. 58 of the GDPR. These powers include the ability for the DPAs to impose corrective actions, such as a temporary or definitive limitation on data processing activities, including a complete ban on data processing, or to order the suspension of data flows to a recipient in a third country.

RegNest Inc and the GDPR

At RegNest Inc, privacy, data protection, and data security are at the very heart of everything we do. We're continuously working to reset the bar for ourselves in the security and data privacy realm, and view the GDPR as an opportunity for the entire industry to come together on this and improve.

GDPR compliance is comprised of many elements. Among others, we are updating our documentation and agreements to align with GDPR requirements. We are also revising our internal policies and procedures to ensure that they adhere to the GDPR standard.

Most of the GDPR compliance elements take place "under the hood" of an organization as they relate to updates on how an organization is processing personal data.

These are some of the steps RegNest Inc is performing for its users in anticipation of the GDPR:

- Perform a gap analysis between the requirements imposed by the Data Protection Directive and the GDPR, as applicable to the company's business operations.
- Review and update internal tools, procedures and policies where necessary.
- Revise data mapping and data inventory practices, and update where necessary, to comply with record retention obligations under the GDPR.
- Perform a dedicated gap analysis of privacy and data protection review tooling to meet the Data Protection Impact Assessment requirements.
- Update approach to international data transfers.
- Update contracts to reflect Art. 28 GDPR obligations as they relate to the company's contracting parties.
- Review and, where necessary, revise relationships with vendors to meet the requirements of the GDPR to ensure that those third parties receive and process personal data in a lawful way.
- Update the company's Privacy Compliance Program with continuous employee training to reflect the changes to be implemented for the GDPR.

The Accountability Principle

RegNest Inc users should consult with their legal professionals to understand the full scope of their compliance obligations under GDPR. As a general rule, if you are an organization that is established in the EU, or if your organization is processing EU individuals' personal data, the GDPR will be applicable to you.

One overriding GDPR principle to keep in mind is the Accountability Principle. The Accountability Principle states that the data controller has to be able to demonstrate that its processing activities are compliant with the data protection principles set forth in the GDPR. The easiest way to demonstrate compliance is by documenting and communicating your GDPR compliance approach.

At RegNest Inc, compliance has been the product of a collaborative effort from many people across our organization, including User Operations, Sales, Engineering, Security and Legal. In our experience, cross-functional partnerships and easy-to-read documentation are incredibly helpful to the overall GDPR compliance process.

Legal Department at info@regnest.com, or by certified mail (return receipt requested) at: RegNest Inc., Attn: Legal Department, 734 Palma Dr, Salinas, CA, 93901 USA


REGNEST