Privacy policy (GDPR compliance)

Resilience Reclaimed
Updated May 2024

---

1. Objective

The objective of this privacy policy is to inform data subjects (the individuals whose data is being processed) about how their personal data is collected, used, protected, and shared by Resilience Reclaimed.

The privacy policy serves several purposes:

1. **Clarify Practices**: We detail our data processing methods and your rights, ensuring you're fully informed.
2. **Establish Trust**: Demonstrating our respect for your privacy underpins trust in our consultancy services.
3. **Adhere to the Law**: We operate in strict compliance with data protection regulations, including GDPR, to fulfill our legal duties.
4. **Maintain Responsibility**: Resilience Reclaimed upholds the commitments made in this policy, answerable to both you and legal entities.
5. **Empower Data Subjects**: You're informed of your rights to manage your personal data and the procedures to exercise them.
6. **Support**: For exercising your rights or privacy-related queries, this policy directs you on how to engage with us effectively.

This policy reflects Resilience Reclaimed's responsible data management, aimed at safeguarding your privacy while ensuring regulatory compliance and transparency.

2. Scope

The scope of the privacy policy is integral to upholding the principles of the GDPR, such as transparency, fairness, and accountability, and it plays a critical role in establishing and maintaining trust between Resilience Reclaimed and those whose data it handles.

The scope of this privacy policy applies to all personal data processing activities of Resilience Reclaimed. It ensures our data handling practices—from collection to disposal—are aligned with data protection laws, and it encompasses:

1. **Applicability**: This policy governs all personal data managed by our consultancy.
2. **Data Collection**: We outline data we collect directly, such as client information, and indirectly through technological means, like cookies.
3. **Processing Purposes**: We process data strictly for service delivery, compliance, or legitimate business operations.
4. **Legal Bases**: Our processing activities are based on clear legal grounds, including consent, contractual requirements, and other lawful justifications.
5. **Disclosure**: We detail circumstances under which we share data with third parties or authorities.
6. **Data Security**: Measures in place to secure data against unauthorized access or breaches are described.
7. **Rights of Data Subjects**: We explain your rights over personal data and the process to exercise them.
8. **Retention Policy**: The criteria determining how long we hold data are clearly stated.
9. **International Transfers**: Where applicable, we outline measures for protecting data in cross-border transfers.
10. **Automated Decision-Making**: We disclose if and how we use automated processes, including profiling.
11. **Contact and Complaints**: Information for privacy-related inquiries, updates to the policy, and avenues for filing complaints.

This policy is fundamental in reinforcing the trust between our clients and Resilience Reclaimed, adhering to GDPR principles such as transparency and accountability.

3. Identity and contact details of the data controller

Data Controller: Erik Rottier – Resilience Reclaimed

Resilience Reclaimed is committed to protecting and respecting your privacy. As the data controller, Resilience Reclaimed is responsible for determining the purposes and means of processing your personal data.

Contact details for data protection: please take contact through the form presented on https://resiliencereclaimed.com/home/contact/

Should you have any questions regarding this privacy policy or our data protection practices, or if you wish to exercise any of your rights under the General Data Protection Regulation (GDPR), please contact us using the details provided above.

We encourage you to reach out to us with any concerns or inquiries you may have pertaining to your personal data and privacy. It is our priority to address and resolve any issues in accordance with the GDPR and to uphold your rights as a data subject.

4. Recipient of personal data

Resilience Reclaimed, led by Erik Rottier, handles all personal data internally and does not routinely engage third-party data processors. However, specific scenarios may require sharing data with external parties:

- **Legal Obligations**: If compelled by legal authorities, we may disclose data as necessary.
- **Operational Service Providers**: For crucial business services like hosting or storage, subcontracted providers are GDPR-compliant, and data is encrypted to maintain confidentiality.
- **Business Changes**: Should corporate structuring events occur, personal data might be part of the assets transitioned with stringent security adherence.

We commit to secure data handling in line with our privacy policy, ensuring transfers are executed with robust protection measures. For detailed information on how we manage and protect your data, or to address concerns about data sharing, refer to the 'Identity and Contact Details of the Data Controller' section.

5. Data sources

Resilience Reclaimed transparently obtains personal data through:

- **Direct Engagement**: Data is collected when you interact with our services, complete forms, or communicate with us.
- **Client Entities**: When rendering consultancy to organizations, we may receive data about individuals from these entities, who are responsible for lawful data acquisition and sharing.

Currently, we do not source data from public records or third-party brokers. If this changes, our policy will reflect such updates, clearly stating the data sources and processing justifications.

We ensure the data we collect serves clear, legitimate purposes, maintaining compatibility with these objectives. In case of indirect data acquisition, we'll inform affected individuals about the data origins and processing intentions, adhering to GDPR requirements.

Details on data use specifics can be found in the 'Personal Information Collected and Relevant Concerns' section, under the 'Purposes of Processing' and 'Legal Basis for Processing' columns.

6. Automated decision making and profiling

At Resilience Reclaimed:

- **Human-Centric Approach**: We exclusively make significant decisions involving your data through human judgement, ensuring personal consideration in every case.
- **No Profiling Activities**: Your data isn't used for automated profiling, which could assess aspects like work performance, economic status, or preferences.

Should our stance on automated decision-making or profiling change, the policy will be revised to detail the processes, impacts, and any requirements for your consent.

7. Data Protection Impact Assessment (DPIA)

Resilience Reclaimed, while typically not engaged in high-risk processing, commits to conducting a Data Protection Impact Assessment (DPIA) as mandated by Article 35 of the GDPR if any processing possibly poses significant risks to personal rights and freedoms.

When DPIA is Necessary:

- Introduction of new technologies.
- Large-scale processing of sensitive data.
- High-risk processing, guided by the Swedish Data Protection Authority and the EDPB.

The DPIA Process:

- We evaluate the processing's necessity and proportion, risks to individuals, and outline measures to mitigate potential risks.
- Documentation of DPIAs is integral to our data processing approach.
- If risks are identified that cannot be adequately addressed, we will consult with the Swedish Data Protection Authority before proceeding with such processing activities.

Our DPIA practice upholds the individual’s rights and adheres to GDPR, exemplifying our commitment to responsible data management.

8. Data location and international transfers

At Resilience Reclaimed:

- **Confined Data Processing**: Sensitive personal data is processed strictly within the EU/EEA, aligning with GDPR's rigorous protections.
- **Selective Third-Party Engagement**: When employing third-party services for contact details processing, we ensure GDPR compliance and prefer EU/EEA-based data management.

International Transfer Safeguards:

- Encrypted transfers and storage.
- Transfers outside EU/EEA only with GDPR-compliant services.
- Use of standard contractual clauses or similar GDPR-endorsed practices.

Our steadfast commitment is to limit international data transfers, opting for EU/EEA-based processing. Transparency is key—we will keep clients informed about their data's location, as detailed in 'Annex 1: Information Technology solutions used and security background'.

9. Data subject rights

As part of Resilience Reclaimed's commitment to GDPR compliance, your rights as a data subject include:

- **Access**: You can request a copy of the personal data we hold about you and understand our processing activities.
- **Rectification**: Should you find inaccuracies in your data, we'll promptly correct them at your request.
- **Erasure**: Also known as the "Right to be Forgotten", you may request deletion of your data where there's no legitimate reason for its continued processing, barring legal obligations.
- **Restriction**: Under certain conditions, you can limit the processing of your data, permitting us only to store it.
- **Portability**: We'll provide your data in a commonly used, machine-readable format, or directly transfer it to another controller if feasible.
- **Objection**: You have the right to oppose processing based on our legitimate interests or for direct marketing.
- **Withdraw Consent**: If our processing is based on your consent, you may withdraw it anytime, impacting only future activities without affecting the previous legality.
- **Complaint**: If you feel your rights under GDPR are violated, you can lodge a complaint with the data protection authority in your EU member state.

To exercise these rights, contact us as outlined in the 'Identity and Contact Details of the Data Controller'.

For verification, we may ask for specific information to confirm your identity. In some instances, like unfounded or excessive requests, we may charge a fee or refuse the request.

Expect a response within one month, with a possibility of extension for complex or numerous requests, in which case we'll keep you informed.

10. Overview of measures taken to protect the security of private data

For a full overview of all measures and how they contribute to the protection of private data please refer to the '*Data and information security Policy'* of Resilience Reclaimed.

11. Data retention policy

Resilience Reclaimed's data retention practices are tailored to balance legal obligations with a commitment to data minimization and privacy:

Organizational Data Retention:

- **Legal and Regulatory Adherence**: Data like identifiable details, contracts, and financial records are kept in line with legal requirements to support tax, legal, and administrative functions.
- **Contract-Related Information**: Additional data necessary for contract fulfillment is deleted three months post-contract to address any residual matters.

Individual Data Retention:
- **Sensitive Data**: Handled only for the contract period and destroyed within three months post-service, with an option for immediate destruction at the individual's request.
- **Early Termination**: Should you choose to halt processing and request data destruction, we may invoice for services rendered up to that point in accordance with the agreement.

Secure Data Destruction:
- Utilizes best practices to ensure complete and irreversible data elimination.

This policy is crafted to meet GDPR standards, affirming our dedication to protecting your data while periodically reassessing to stay current with legal and operational shifts.

12. Policy revision and updates

This Policy will be reviewed and updated annually or as necessary to adapt to changes in the regulatory frameworks.

13. Personal information collected and relevant concerns

In line with GDPR principles, Resilience Reclaimed follows the data minimization principle. Personal information collected is kept to the minimum necessary for the proper development of services and is based on common sense and legal compliance.

Working with organisations: Organisational Resilience, Business Continuity and Forecasting activities

Type of information collected	***Purposes of processing***	***Legal basis for processing***	***Phase***	***How is data collected***	***Data collection based on***
Contact details (e.g., email, phone number)	*Respond to inquiries and provide information about services requested by the potential client*	*Legitimate interests (Article 6(1)(f) GDPR) - Processing is necessary to respond to the individual's inquiry and provide information about services they have expressed potential interest in*	*Initial Inquiry*	*Contact form on the website of Resilience Reclaimed*	*Individuals provide their contact details when making an inquiry, indicating their interest in potentially entering into a contract. The privacy notice provided alongside the contact form explains the purpose and legal basis for processing this data*
Identifiers (name, email address, telephone number, conference call handles)	*Communication with potential clients to provide/ receive additional information and preparation for contractual agreement*	*Legitimate interests (Article 6(1)(f) GDPR) - Processing is necessary for the purpose of pursuing Resilience Reclaimed's legitimate business interests in establishing a business relationship*	*Pre-contractual communications*	*Through direct contacts with staff and colleagues through e-mail, telephone, conference call, face-to-face meetings, etc*	*The Privacy Policy detailing the legitimate interests and data subjects' rights is explicitly presented and acknowledged during the first communication*
Identifiers (name, email address, telephone number, conference call handles, general location of residence of individuals)	*Data/ information necessary to fulfil the expectations and conditions of the client, or administrative contractual agreement*	*Contractual necessity (Article 6(1)(b) GDPR) - Processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract*	*Contract Execution*	*Through direct contacts with staff and colleagues through e-mail, telephone, conference call, face-to-face meetings, etc*	*The processing of data for contractual purposes is agreed upon within the contractual terms, as outlined in the Privacy Policy provided before the contract is signed*
Identifiers (name, email address, telephone number, conference call handles)	*Data/ information necessary for management of administrative/ legal issues related to the contract*	*Legal obligation (Article 6(1)(c) GDPR) - Processing is necessary for compliance with legal obligations to which the data controller is subject (e.g., tax law)*	*Contract Fulfilment*	*Through direct contacts with staff and colleagues through e-mail, telephone, conference call, face-to-face meetings, etc*	*The necessity for compliance with legal obligations is explicitly communicated through our Privacy Policy, which data subjects have access to and agree to as part of the contractual terms*
Contract details (e.g., contract terms, dates, parties involved),	*To comply with legal obligations such as tax reporting, audit*	*Compliance with a legal obligation (Article 6(1)(c) GDPR) - compliance with a legal obligation. legal*	*Contract Execution and*	*Directly from the relevant staff members or from the*	*Legal requirement: statutory or regulatory mandates that necessitate the collection of this*

Type of information collected	***Purposes of processing***	***Legal basis for processing***	***Phase***	***How is data collected***	***Data collection based on***
financial records (e.g., invoices, payment records), staff member identifiers necessary for legal obligations (e.g., names, position, contact details for tax reporting)	*requirements, and regulatory compliance*	*requirement of authorities to process and retain this data*	*Post-contractual period*	*organisation's documentation during the performance of the contract*	*information for compliance purposes.* *The statutory or regulatory retention period is clearly stated in the Privacy Policy, which also informs the data subject of their rights regarding data retention*
Contact details (e.g., email, phone number)	*To send occasional communications for additional support, refresher opportunities, or new services/offers*	*Consent (Article 6(1)(a) GDPR) and Legitimate interests (Article 6(1)(f) GDPR) - Processing is based on explicit consent obtained for marketing communications and the legitimate interests of maintaining business relationships*	*Post-contract Relationship Management*	*Provided by the client during the client relationship*	*Clients provide explicit consent for marketing communications and are informed of their right to withdraw consent and object to processing based on legitimate interests, as detailed in our Privacy Policy*

According to our legal obligations, we are required to retain the contract details for a period of seven years. Once this period has elapsed, the data will be securely disposed of.

During the retention period, all collected data and information will be safeguarded in accordance with the '*Data and Information Security Policy*' of Resilience Reclaimed.

We value the trust and relationship we build with clients, and any post-contract communication will be minimal and non-intrusive. This type of correspondence will be limited to a maximum of twice per year, ensuring that it is relevant and offers genuine value, such as additional support opportunities, refresher sessions, or information about new services that may interest you. We understand the importance of your privacy and attention, and endeavour to respect that in every interaction. Should you prefer not to receive these communications, you have the right to opt out at any time, and your preferences will be promptly honoured.

Personal and Household Resilience

For work with organisations, personal data processing is generally limited to identifiers associated with individual staff members. However, when focusing on the resilience of individual persons and their households, the nature of the information is inherently more personal and may include sensitive data. Identifying vulnerabilities is a critical aspect of our service, as it enables us to pinpoint and prioritize measures that can strengthen resilience for the individual or household.

While identifiers associated with individuals such as names and contact details can be processed on the legal basis of legitimate interests or contractual necessity, the GDPR requires explicit consent for the processing of special categories of personal data, also known as sensitive data. This includes information related to health, economic situation, or other aspects that could reveal vulnerabilities.

To ensure the privacy and protection of individual identities, sensitive information is collected and managed with careful regard to confidentiality. During assessments, data is recorded on paper without direct links to personal identifiers like names or contact details. Such an approach is aligned with GDPR-compliant pseudonymisation techniques—meaning that, while the data does not directly reveal individual identities, there exists the potential to re-associate it with specific individuals if necessary.

Pseudonymised data is still subject to GDPR regulations, and Resilience Reclaimed is committed to maintaining high data and information protection standards. This information is strictly used to generate reports that identify potential vulnerabilities and propose targeted measures to bolster resilience.

To bridge the gap between anonymised insights and the need to provide customised services, each client's sensitive data is assigned a unique numeric identifier. The key for reconnecting pseudonymised data with individual clients is securely encrypted and stored separately. Access to this key is highly restricted, reserved for instances where re-identification is essential—such as when clients exercise their rights under GDPR to access or modify their data.

Type of information collected	***Purposes of processing***	***Legal basis for processing***	***Phase***	***How is data collected***	***Data collection based on***
Contact details (e.g., email, phone number)	*Respond to inquiries and provide information about services requested by the potential client*	*Legitimate interests (Article 6(1)(f) GDPR): The processing is necessary for the purposes of legitimate interests pursued by the controller, which is to establish communication with the potential client*	*Initial Inquiry*	*Contact form on website of Resilience Reclaimed*	*By submitting the contact form, individuals initiate contact indicating interest in our services. Our Privacy Notice, which outlines these processes, is available to read before submission*
Identifiers (name, email address, telephone number, conference call handles)	*Communication with potential clients to provide/ receive additional information and preparation for contractual agreement*	*Legitimate interests (Article 6(1)(f) GDPR) - Processing is necessary for the purpose of pursuing legitimate business interests, namely establishing a business relationship. It's presumed that individuals involved have an expectation of such communication*	*Pre-contractual communications*	*Through direct contacts with private persons and household members through e-mail, telephone, conference call, chat, face-to-face contact, etc*	*The Privacy Policy detailing the legitimate interests and data subjects' rights is explicitly presented and acknowledged during the first communication*
Identifiers (name, email address, address, telephone number, conference call handles, general	*Data/ information necessary to fulfil the expectations and conditions of the private client, or*	*Contractual necessity (Article 6(1)(b) GDPR) - Processing is necessary for the performance of a contract to which the data subject is party, or to take steps at*	*Contract Execution*	*Through direct contacts with private persons and household members through e-mail, telephone,*	*Data processing for contractual administration is outlined in our Privacy Policy provided at the onset of our business relationship*

Type of information collected	***Purposes of processing***	***Legal basis for processing***	***Phase***	***How is data collected***	***Data collection based on***
location of residence of individuals)	*administrative contractual agreement*	*the request of the data subject prior to entering a contract*		*conference call, chat, face-to-face contact, etc*	
Sensitive data related to vulnerabilities and capacities: health indicators, economic factors, personal skills, etc. (exact data types may vary based on individual assessment needs)	*To conduct an in-depth assessment and analysis of the client's vulnerabilities and capacities to identify and prioritize measures to strengthen resilience*	*Explicit consent (Article 9(2)(a) GDPR): The data subject has given explicit consent to the processing of those personal data for the specified purposes*	*Contract Fulfilment*	*Direct interviews and consultations with private persons and household members* *Analysis of secondary sources (public records, local risk assessments)* *Observational data collection in publicly accessible areas*	*Written consent obtained at the start of the business relationship or at the time of data collection, ensuring it is informed, specific, and freely given; clients retain the option to withdraw consent at any time*
Contract details, financial records, identifiers necessary for legal obligations (e.g., names, position, contact details for tax reporting)	*To comply with legal obligations such as tax reporting, audit*	*Compliance with a legal obligation (Article 6(1)(c) GDPR) - compliance with a legal obligation. legal requirement of authorities to process and retain this data*	*Contract execution and post-contractual period follow-up*	*Through direct contacts with private persons through e-mail, telephone, conference call, chat, face-to-face contact, etc*	*Legal requirement: statutory or regulatory mandates that necessitate the collection of this information for compliance purposes.* *The statutory or regulatory retention period is clearly stated in the Privacy Policy, which also informs the data subject of their rights regarding data retention*
Identifiers (name, email address, telephone number, conference call handles)	*Contact information necessary for potential follow-up with client after termination of contract*	*Legitimate interests (Article 6(1)(f) GDPR) - Processing is necessary for the purpose of pursuing legitimate business interests, including maintaining business relationships and potential future contracts*	*Post-contract*	*Through direct contacts with private persons through e-mail, telephone, conference call, chat, etc*	*By entering into a contract with Resilience Reclaimed, you acknowledge that we may retain your contact details for potential follow-up post-contract, as described in our Privacy Notice*

14. Use of Cookies and Similar Technologies

Resilience Reclaimed employs cookies for website functionality and user experience enhancement on https://resiliencereclaimed.com.

Cookies Explained: Cookies are small files placed on your device to ensure the website's essential operations and to gather anonymous usage statistics.

Cookie Categories used at the time of the review of this policy (may 2024):

- **Essential**: Crucial for website navigation and core functions.
- **Statistics**: Collect anonymous data to understand user interactions.

For a detailed list of active cookies, refer to 'Annex 2: Cookies in Use'.

Your Choices:

- **Consent**: We request your permission for non-essential cookies on your first visit.
- **Management**: Modify browser settings to control cookie use or withdraw consent through our website's switch icon.

Third-Party Cookies:

- Note that external services may set cookies beyond our control; manage these via browser settings.

Policy Updates:

- We will post any future alterations to our cookie policy on this page.

For queries or assistance regarding our cookie use, please reach out through our contact page https://resiliencereclaimed.com/home/contact/.

Annex 1: Information Technology solutions used and security background

At Resilience Reclaimed, I, Erik Rottier, am the sole proprietor and exclusive user of all IT solutions detailed below. I personally manage access controls and ensure no external parties can access these systems or the data within.

For a comprehensive view of our data security management, please consult the 'Data and Information Security Policy' of Resilience Reclaimed.

GDPR Compliance Review Process:

- Conducted in tandem with policy reviews, assessing each software and service for data protection risks.
- Factors considered include data type, software security features, and processing environment changes.

Adherence to 'Privacy by Design':

- Privacy Impact Assessments (PIAs) performed when updating systems.
- Data minimization by collecting only necessary data for specified purposes.
- Encryption of sensitive data to prevent unauthorized access.
- Anonymization of data wherever possible to prevent individual identification.
- Restricted data access based on necessity.
- Privacy-focused user interface design, including clear privacy settings and consent forms.
- Regular process reviews to stay abreast of technological and regulatory developments.

Assumptions for Data Security:

- Software and services are assumed to be free from exploitable bugs or vulnerabilities; see 'Data and Information Security Policy' for more details.
- No backdoors exist in our software/services that would allow unauthorized access to the data by any actors.

Please note, this annex is a living document and will be updated to reflect the current use of technology and risk assessments in line with our commitment to data privacy and security.

Software/ service	***Location of data***	***Background concerning data and IT security/ GDPR compliance***
Microsoft 365 Business Professional	• *Computer*	• *The Office package operates locally on the computer without automatic cloud integration or syncing capabilities. Documents and files are securely saved on local and on-site external storage or encrypted on Proton Drive (part of the Proton Business suite, see below)* • *For online collaboration and communication (chat/videoconferencing), MS Teams is used. Microsoft Teams is built on Microsoft 365, ensuring advanced security and compliance with GDPR, including data encryption, audit capabilities, data loss prevention, and strict adherence to privacy standards* • *For translation, Microsoft Translator is used; this service is GDPR compliant, offering 'No Trace' translations where data is not stored persistently, and there is no data sharing with third parties*
iWork	• *Computer*	• *Apple's alternative to Microsoft Office* • *Operates locally on the computer without automatic cloud integration or syncing capabilities* • *iWork used locally for presentations with potential sensitive data encrypted* • *Documents and files securely saved on local and on-site external storage or encrypted on Proton Drive (part of Proton Business suite)*
Preview	• *Computer*	• *Operates locally on the computer without automatic cloud integration or syncing capabilities* • *Documents and files securely saved on local and on-site external storage or encrypted on Proton Drive (part of Proton Business suite)*
Omnigraffle	• *Computer*	• *Operates locally on the computer without automatic cloud integration or syncing capabilities*

Software/ service	***Location of data***	***Background concerning data and IT security/ GDPR compliance***
		• *Omnigraffle is not used for sensitive personal data* • *Documents and files securely saved on local and on-site external storage or encrypted on Proton Drive (part of Proton Business suite)*
Mozilla Firefox	• *Not applicable as no sensitive data is handled by Firefox*	• *Web browsing managed locally* • *VPN in use* • *Extensions for security and privacy: Trafficlight (part of Bitdefender), uBlock and DuckDuckGo Privacy Essentials* • *Firefox processes and stores browsing data locally and offers robust privacy settings, but does not control third-party services' data handling through its browser interface* • *Third-party services accessed via Firefox are responsible for their own GDPR compliance and data protection; end-to-end encryption is service-dependent* • *Mozilla advocates for privacy, providing features like HTTPS support to enhance user data security*
Apple Mail	• *Computer*	• *E-mail addresses with the extension @resilientwash.org are accessed through Apple Mail.* • *All e-mail addresses with the extension @resiliencereclaimed.com are accessed through the Proton Business suite (see below for details).*
iShredder	• *Not applicable as data is not handled directly but overwritten*	• *iShredder executes secure data deletion processes locally on the device, utilizing industry-standard erasure algorithms without requiring external server connectivity* • *Data wiping reliably removes selected data from storage* • *iShredder provides GDPR-compliant data deletion (information provided by software provider)* • *iShredder provides detailed deletion reports that are archived*
Proton Business	• *Switzerland*	• *Switzerland is aligned with European GDPR standards* • *Services used are Proton Mail (e-mail service), Proton Drive (cloud storage), Proton Pass (password manager) and Proton Calendar (calendar)* • *All services from Proton Business are end-to-end encrypted* • *In addition to Proton's native end-to-end encryption, sensitive data stored on the Cloud service Proton Drive will be encrypted to military level AES 256-bit using the CloudAshur system*
CloudAshur, DiskAshur	• *Computer hard drive and external storage*	• *Sensitive data is natively stored in encrypted form on the HD of the Mac Desktop and Laptop* • *In addition to this, sensitive data stored on the computers will be encrypted to military level AES 256-bit using the CloudAshur system* • *Sensitive data stored externally will be either stored on a DiskAshur unit encrypted to military level AES 256-bit, or stored on external storage encrypted to military level AES 256-bit using the CloudAshur system*

Annex 2: Cookies in use on the website
For the Resilience Reclaimed website https://resiliencereclaimed.com/

Source of report : Scan by Cookiebot (Usercentrics)
Date of report : 08 May 2023

Cookie scan report

Summary
Scan date: 08/05/2024
Domain name: resiliencereclaimed.com
Server location: United States
Cookies, in total: 5

Scan result
5 cookies were identified.

Category: Necessary (4)

Necessary cookies help make a website usable by enabling basic functions like page navigation and access to secure areas of the website. The website cannot function properly without these cookies.

COOKIE NAME	PROVIDER	TYPE	EXPIRY
CookieConsent	resiliencereclaimed.com	HTTP	1 year
First found URL: https://resiliencereclaimed.com/ **Cookie purpose description:** Stores the user's cookie consent state for the current domain **Initiator:** Script tag, page source line number 24 **Source:** https://consent.cookiebot.com/uc.js **Data is sent to:** Ireland (adequate) Adequate country under GDPR (EU)			
rc::a	gstatic.com	HTML	Persistent
First found URL: https://resiliencereclaimed.com/sv/home-svenska/kontakt/ **Cookie purpose description:** This cookie is used to distinguish between humans and bots. This is beneficial for the website, in order to make valid reports on the use of their website. **Initiator:** Script tag, page source line number 749 **Source:** https://www.google.com/recaptcha/api.js?onload=wpformsRecaptchaLoadrender=explicit **Data is sent to:** United States (adequate) Adequate country under GDPR (EU)			
rc::c	gstatic.com	HTML	Session
First found URL: https://resiliencereclaimed.com/sv/home-svenska/kontakt/ **Cookie purpose description:** This cookie is used to distinguish between humans and bots. **Initiator:** Script tag, page source line number 749 **Source:** https://www.google.com/recaptcha/api.js?onload=wpformsRecaptchaLoadrender=explicit **Data is sent to:** United States (adequate)			

Adequate country under GDPR (EU)

wpEmojiSettingsSupports	resiliencereclaimed.com	HTML	Session

First found URL: https://resiliencereclaimed.com/
Cookie purpose description: This cookie is part of a bundle of cookies which serve the purpose of content delivery and presentation. The cookies keep the correct state of font, blog/picture sliders, color themes and other website settings.

Initiator: Page source line number 55
Source: Inline script

Data is sent to: United States (adequate)

Adequate country under GDPR (EU)

Category: Statistics (1)

Statistic cookies help website owners to understand how visitors interact with websites by collecting and reporting information anonymously.

COOKIE NAME	PROVIDER	TYPE	EXPIRY
g.gif	pixel.wp.com	Pixel	Session

First found URL: https://resiliencereclaimed.com/
Cookie purpose description: Registers statistical data on users' behaviour on the website. Used for internal analytics by the website operator.

Initiator: Page source line number 843
Source: Inline script

Data is sent to: United States (adequate)

Adequate country under GDPR (EU)