



UK Operational Resilience Framework Mapping

The UK's operational resilience framework is a set of policies designed to ensure financial firms can prevent, withstand, and recover from disruptions to critical business services. As part of the UK operational resilience framework established and enforced by the Prudential Regulation Authority (PRA), the Financial Conduct Authority (FCA), and the Bank of England supporting Supervisory Statements (“SS”) have been published. SS are guidelines issued by UK regulators, particularly the PRA, to clarify how financial firms should meet their regulatory obligations.

This document is designed to help regulated firms supervised by the PRA (“Regulated Entity”) to understand where the rules and obligations of the PRA's Operational Resilience policy under “ **SS2/21 Outsourcing and third party risk management**” (the “Framework”) are addressed in Cloudflare’s terms and policies, in particular the Enterprise Subscription Terms of Service (“ToS”) and its appendices as well as the Order Form.

Capitalized terms will have the meanings set forth in the ToS and referenced documents therein. If not referenced in those documents, they shall have the meaning given by the Framework.

This mapping focuses on the following Sections of the Framework: Chapter 6 - Outsourcing agreements, Chapter 7 - Data Security, Chapter 8 - Access, audit and information rights, Chapter 9 - Sub-outsourcing and Chapter 10 - Business continuity and exit plans.

#	Framework reference	Cloudflare terms and policy reference
6	Outsourcing agreements	
1	6.1 In line with Article 31(3) of MODR (banks) and 274(3)(c) of the Solvency II Delegated Regulation (insurers), all outsourcing arrangements must be set out in a written agreement.	The Cloudflare Agreement is a written contract between the parties either signed or incorporated in the Service Order Form which is signed by both parties.
2	6.2 Where there is a master service agreement that allows firms to add or remove certain services, each outsourced service should be appropriately documented, although not necessarily in a separate agreement.	All purchased Services are described in the respective Order Form that will be signed by the Customer. Additional Services are purchased via signed Order Form or Insertion Order.

3	<p>6.3 Firms should ensure that written agreements for non-material outsourcing arrangements include appropriate contractual safeguards to manage and monitor relevant risks. Moreover, regardless of materiality, firms should ensure that outsourcing agreements do not impede or limit the PRA's ability to effectively supervise the firm or outsourced activity, function, or service.</p>	<p>Cloudflare grants audit, access and information rights to Regulated Entities and supervisory authorities. In the Customer dashboard you can find the latest SOC 2 audit reports and we provide summaries of different certification audits upon request.</p> <p>The ToS also incorporate by reference the Customer Support and Service Level Agreement ("SLA"), current version to be found at: https://www.cloudflare.com/enterprise-support-sla/.</p>
Material outsourcing agreements		
4	<p>6.4 Written agreements for material outsourcing should set out at least:</p>	
5	<ul style="list-style-type: none"> • a clear description of the outsourced function, including the type of support services to be provided; 	<p>The Order Form specifies the Services that the Customer is purchasing and has attached the applicable Service-Specific Terms that can be found also under: https://www.cloudflare.com/service-specific-terms-overview. The Service-Specific Terms contain details about the products and their functions. Furthermore, the ToS refer to the Documentation, which is defined as all online user manuals, developer documentation, and other technical materials relating to the Services made available to Customer by Cloudflare. The Documentation can be found in the Customer dashboard after login.</p> <p>The ToS also incorporates by reference the Customer Support and Service Level Agreement ("SLA"), current version to be found at: https://www.cloudflare.com/enterprise-support-sla/. The SLA clearly set out the details of the support provided.</p>
6	<ul style="list-style-type: none"> • the start date, next renewal date, end date, and notice periods regarding termination for the service provider and the firm; 	<p>Start Date and End Date are specified in the Order Form. Renewal Dates and notice periods are defined in the ToS under Section 11.</p>

7	<ul style="list-style-type: none"> the governing law of the agreement; 	Governing Law is stated under 12.1 of the ToS.
8	<ul style="list-style-type: none"> the parties' financial obligations; 	The Fees are stated in the respective Order Form and the payment terms under Section 3 of the ToS.
9	<ul style="list-style-type: none"> whether the sub-outsourcing of a material function or part thereof is permitted and, if so, under which conditions; 	<p>Section 4 our DPA explains when subprocessing and working with subcontractors that could have access to personal data is allowed.</p> <p>Under section 4.4 of the DPA there is a reference to the website where a detailed list of all sub Processors is contained (https://www.cloudflare.com/gdpr/subprocessors/). This list specifies the name, activity and the location of the processing.</p>
10	<ul style="list-style-type: none"> the location(s), ie regions or countries, where the material function or service will be provided, and/or where relevant data will be kept, processed, or transferred, including the possible storage location, and a requirement for the service provider to give reasonable notice to the firm in advance if it proposes to change said location(s); 	<p>Under section 4.4 of the DPA the reference to the website where a detailed list of all sub Processors is contained (https://www.cloudflare.com/gdpr/subprocessors/). This list specifies the name, activity and the location of the processing.</p> <p>Under 4.4 the procedure in case of changes is described. All changes to the sub-Processor list are done at least thirty (30) days prior to the commencement of the new or replaced sub Processor and the Customer has an objection right.</p> <p>Cloudflare runs an anycast network to ensure a fast and reliable service. Details can be found in the following resources here:</p> <ul style="list-style-type: none"> Cloudflare Anycast Network Load Balancing without Load Balancers Cloudflare Global Network
11	<ul style="list-style-type: none"> provisions regarding the accessibility, availability, integrity, confidentiality, privacy, and safety of relevant data (see Chapter 7); 	<p>The SLAs (https://www.cloudflare.com/enterprise-support-sla/ and https://www.cloudflare.com/r2-service-level-agreement/) contain Cloudflare's commitment regarding availability of the Services, which is 100%.</p> <p>Authenticity, integrity and confidentiality is addressed in the DPA (https://www.cloudflare.com/cloudflare-customer-dpa/) and in particular in its Annex 2 where the technical and organizational measures that Cloudflare has implemented to keep Customer data secure are set out.</p> <p>Furthermore, the Information Security Exhibit (https://www.cloudflare.com/security-exhibit/) outlines the security requirements that Cloudflare maintains to ensure the security, confidentiality, integrity, and availability of Customer Data.</p> <p>All aforementioned documents are incorporated into the ToS.</p> <p>In section 8 of the ToS itself (https://www.cloudflare.com/enterpriseterms/) the</p>

		<p>confidentiality obligations for Cloudflare and the Customer are stated.</p> <p>From the beginning, Cloudflare has built its systems to ensure that data is kept private and secure. The security we apply is fully in line with, and in many cases goes well beyond the requirements of the General Data Protection Regulation (GDPR).</p> <p>For details regarding our comprehensive certifications we maintain you can visit our trust hub: https://www.cloudflare.com/trust-hub/compliance-resources/</p>
12	<ul style="list-style-type: none"> the right of the firm to monitor the service provider's performance on an ongoing basis (this may be by reference to KPIs); 	<p>The Cloudflare SLAs can be found under: https://www.cloudflare.com/enterprise-support-sla/. They contain remedy regulations and also a crediting process in case SLAs are not met.</p> <p>You are able to check the status of our Services anytime online under https://www.cloudflarestatus.com/.</p>
13	<ul style="list-style-type: none"> the agreed service levels, which should include qualitative and quantitative performance criteria and allow for timely monitoring, so that appropriate corrective action can be taken if these service levels are not met; 	<p>Please see row 12</p>
14	<ul style="list-style-type: none"> the reporting obligations of the service provider to the firm, including a requirement to notify the firm of any development that may have a material or adverse impact on the service provider's ability to effectively perform the material function in line with the agreed service levels and in compliance with applicable laws and regulatory requirements; 	<p>Cloudflare will, without undue delay, report to Customer any development that may have a material impact on Cloudflare's ability to effectively carry out the Services in line with the agreed Service Levels and in compliance with Applicable Laws and regulatory requirements and provide Customer regular updates during the period that the Services are disrupted.</p> <p>In addition, Cloudflare will promptly notify Customer if Cloudflare discovers or is notified of a breach of security, which results in unauthorized access, acquisition, disclosure, or use relating to any Customer Data ("Data Breach"). Cloudflare will investigate the Data Breach; mitigate the effects of the Data Breach; and perform post-incident assessments and report on the results of such assessment(s) to Customer. These obligations in case of an Information Security Incident are also stated in our Information Security Addendum under section 9 (https://www.cloudflare.com/security-exhibit/).</p>
15	<ul style="list-style-type: none"> whether the service provider should take out mandatory insurance against certain risks and, if applicable, the level of insurance cover requested; 	<p>Cloudflare maintains insurance cover against a number of identified risks.</p>

16	<ul style="list-style-type: none"> the requirements for both parties to implement and test business contingency plans. For the firm, these should take account of their impact tolerances for important business services. Where appropriate, both parties should commit to take reasonable steps to support the testing of such plans; 	<p>Cloudflare will maintain and annually update a comprehensive business continuity framework to ensure that we are able to minimize disruption to the performance of our obligations under the Agreement. Cloudflare notifies the Customer without undue delay if we identify a defect in our Business Continuity Plan which would materially affect service provisioning. Cloudflare will periodically test the Business Continuity Plan to ensure that it minimizes the risk of disruption or severe impact on the Services.</p>
17	<ul style="list-style-type: none"> provisions to ensure that data owned by the firm can be accessed promptly in the case of the insolvency, resolution, or discontinuation of business operations of the service provider; 	<p>Cloudflare enables the Customer to access and export its data throughout the duration of the contract. Customer can access their logs through the dashboard after login and can use Logpush to save the data for as long as they want in data storage of their choice. Please also see row 24.</p>
18	<ul style="list-style-type: none"> the obligation of the service provider to co-operate with the PRA and the Bank, as resolution authority, including persons appointed to act on their behalf (see Chapter 8, including the section on the Bank's and PRA's information gathering and investigatory powers); 	<p>Cloudflare will cooperate with supervisory authorities, resolution authorities and their appointees exercising their audit, information and access rights.</p>
19	<ul style="list-style-type: none"> for banks, a clear reference to the Bank's resolution powers, especially under sections 48Z and 70C-D of the Banking Act 2009 (implementing Articles 68 and 71 of Directive 2014/59/EU (BRRD)), and in particular, a description of the 'substantive obligations' of the written agreement in the sense of Article 68 of that Directive); 	<p>Cloudflare recognizes that Regulated Entities and any resolution entity must be able to carry on business during resolution. To provide support through resolution, Cloudflare commits to continue providing the Services during resolution as required by the BRRD.</p>
20	<ul style="list-style-type: none"> the rights of firms and the PRA to inspect and audit the service provider with regard to the material outsourced function (see Chapter 8); 	<p>Cloudflare grants the Customer an audit right which is stated under section 5 of the DPA in detail.</p> <p>Cloudflare is a highly audited entity, and commits to comply with and maintain the following certifications during the term of the Agreement:</p> <ul style="list-style-type: none"> ISO/IEC 27001 (Information Security Management Systems) ISO/IEC 27701 (ISO privacy certification) ISO/IEC 27018 (Cloud Privacy)

		<ul style="list-style-type: none"> ● PCI DSS ● SOC 2 Type II ● C5 Type 2 <p>Customers can request Cloudflare’s comprehensive yearly audit report which is also available on Customer’s dashboard.</p> <p>If any necessary information shall be missing or not sufficient to comply with the audit requirements under Framework, the Customer is entitled to conduct an audit. We fully cooperate and grant the resolution authority, as required under the Framework, unrestricted audit and access rights to relevant information required by the resolution authority. The scope, procedure and other details of any audit are determined in the Agreement.</p>
21	<ul style="list-style-type: none"> ● if relevant: 	
22	<ul style="list-style-type: none"> o appropriate and proportionate information security related objectives and measures, including requirements such as minimum ICT security requirements, specifications of firms’ data lifecycles, and any requirements regarding to data security (see Chapter 7), network security, and security monitoring processes; and 	<p>Our Information Security Exhibit (https://www.cloudflare.com/security-exhibit/) outlines the security requirements that Cloudflare maintains to ensure the security, confidentiality, integrity, and availability of Customer data.</p> <p>Cloudflare is highly certified. Please see here all the certifications we maintain including those under which we are audited regularly: https://www.cloudflare.com/trust-hub/compliance-resources/</p>
23	<ul style="list-style-type: none"> o operational and security incident handling procedures, including escalation and reporting; and 	<p>Cloudflare will promptly notify Customer if Cloudflare discovers or is notified of a breach of security, which results in unauthorized access, acquisition, disclosure, or use relating to any Customer Data (“Data Breach”). Cloudflare will investigate the Data Breach; mitigate the effects of the Data Breach; and perform post-incident assessments and report on the results of such assessment(s) to Customer. These obligations in case of an Information Security Incident are also stated in our Information Security Addendum under section 9 (https://www.cloudflare.com/security-exhibit/).</p>

		In the event the Customer purchases a dedicated Technical Account Manager service, the escalation management, communicating resolution and compiling routine summary report for the Customer shall be made available through such services.
24	<ul style="list-style-type: none"> ● termination rights and exit strategies covering both stressed and non-stressed scenarios, as specified in Chapter 10. As in the case of business contingency plans, both parties should commit to take reasonable steps to support the testing of firms' termination plans. Firms may elect to limit contractual termination rights to situations such as: 	<p>Cloudflare enables the Customer to access and export its data throughout the duration of the contract. Customer can access their logs through the dashboard after login and can use Logpush to save the data for as long as they want in data storage of their choice.</p> <p>Cloudflare understands that financial entities are highly conscious about reliability and business continuity and therefore require further contractual commitments in this respect. Cloudflare therefore agrees to continue to provide its Services for a predefined post termination period after the end of the Term upon request.</p>
25	<ul style="list-style-type: none"> ○ material breaches of law, regulation, or contractual provisions; 	<p>Regulated Entities may terminate the Agreement if Cloudflare is in breach of the Agreement or Law and has not remedied this breach within the set reasonable cure period.</p> <p>Furthermore, Regulated Entities are given special termination rights if instructions to terminate the Agreement with immediate effect are given by a resolution authority of Customer.</p>
26	<ul style="list-style-type: none"> ○ those that create risks beyond their tolerance; or 	Please see row 25.
27	<ul style="list-style-type: none"> ○ those that are not adequately notified and remediated in a timely manner. 	Please see row 25.

28	<p>6.5 If an outsourced service provider in a material outsourcing arrangement is unable or unwilling to contractually facilitate a firm’s compliance with its regulatory obligations and expectations, including those in paragraph 6.4, firms should make the PRA aware of this.</p>	<p>If there are any changes within our Services or Agreement that prevent Customer from complying with its mandatory statutory obligations, Customer has a termination right with immediate effect.</p> <p>We are of course committed to working with Regulated Entities to provide necessary support and assistance and to address the impact of changes in law or regulation.</p>
7 Data security		
29	<p>7.11 The PRA expects firms to implement robust controls for data-in-transit, data-in-memory, and data-at-rest. Depending on the materiality and risk of the arrangement, these controls may include a range of preventative and detective measures, including but not necessarily limited to:</p>	
30	<ul style="list-style-type: none"> • configuration management. This is a particularly important measure, as for example, in the context of cloud, misconfiguration of cloud services can be a major cause of data breaches; 	<p>Customers can choose to use the following tools and practices provided by Cloudflare to assist them with configuration management:</p> <ul style="list-style-type: none"> • Cloudflare Dashboard and API allows to centrally configure and manage security and performance settings across customers domains and applications. Permissions can be scoped using API tokens and Role-Based Access Control (RBAC). • Cloudflare Terraform Provider enables customers to manage Cloudflare resources through Infrastructure as Code (IaC). Customers can define, version-control, and audit their Cloudflare configurations in a declarative model. • Cloudflare Zero Trust policies can be managed declaratively and enforced globally. • Audits Logs and Alerts are available to customers to provide visibility into

		<p>configuration changes, including who made them and when. These can be exported into SIEM tools for monitoring and detection.</p> <ul style="list-style-type: none"> Automated Validation and Safe Deployment practices are used internally by Cloudflare to ensure that configuration changes undergo review, testing, and phased rollout across its global network.
31	<ul style="list-style-type: none"> encryption and key management; 	<p>Cloudflare encrypts customer data at rest and in transit by default. Cloudflare’s IT Security Measures can be found under Annex 2 of the DPA (https://www.cloudflare.com/cloudflare-customer-dpa/) and under the Information Security Exhibit (https://www.cloudflare.com/security-exhibit/), both incorporated in the ToS.</p> <p>TLS 1.0 is the version that Cloudflare sets by default for all customers using certificate-based encryption. As a general rule, Cloudflare recommends setting TLS to 1.3, as it will provide the best security.</p> <p>Customers can choose the following encryption and key management tools provided by Cloudflare:</p> <ul style="list-style-type: none"> Automatic TLS/SSL encryption is enabled by default for data in transit between end-users and Cloudflare’s edge, and between Cloudflare and customer origin servers. Cloudflare manages certificate issuance, rotation, and renewal through Cloudflare dashboard and API. Keyless SSL allows customers to use Cloudflare’s global edge network while retaining control of their private TLS keys within their own infrastructure. Keys never leave the customer’s environment and can be integrated with Hardware Security Modules (HSMs). Geo Key Manager enables customers to restrict the geographical locations where private TLS keys are stored and used within Cloudflare’s data centers.

32	<ul style="list-style-type: none"> identity and access management, which should include stricter controls for individuals whose role can create a higher risk in the event of unauthorised access, (eg systems administrators). Firms should be particularly vigilant about privileged accounts becoming compromised as a result of phishing attacks and other leaking or theft of credentials in line with paragraph 31 of the EBA ICT GL; 	<p>Cloudflare’s measures for user identification and authorization Security Measures can be found under Annex 2 of the DPA (https://www.cloudflare.com/cloudflare-customer-dpa/) and under the Information Security Exhibit (https://www.cloudflare.com/security-exhibit/), both incorporated in the ToS.</p> <p>You can choose to use the following tools provided by Cloudflare to assist you with identity and management:</p> <ul style="list-style-type: none"> Cloudflare Access (Zero Trust) provides identity-based access controls for applications, resources, and services. Policies can be enforced based on user identity, device posture, location, and multifactor authentication. Cloudflare Gateway and Browser Isolation allow customers to enforce least-privilege access and reduce phishing risk by controlling how users interact with the internet and applications, limiting exposure of credentials. Role-Based Access Control (RBAC) in the Cloudflare dashboard and API allows organizations to assign granular roles and permissions to users. API tokens with scope permissions enable customers to programmatically manage Cloudflare resources with fine-grained access rights. Single Sign-On (SSO) integrations allow customers to connect to Cloudflare’s Zero Trust platform with their existing identity provider (IdP) providing centralized identity management. Audit logs provide visibility into all configuration changes and access attempts for privileged accounts.
33	<ul style="list-style-type: none"> the ongoing monitoring of ‘insider threats’, (ie employees at the firm and at the third party who may misuse their legitimate access to firm data for unauthorised purposes maliciously or inadvertently). The term ‘employee’ should be construed broadly for these purposes and may include contractors, secondees, and sub-outsourced service providers (see Chapter 9); 	<p>Cloudflare recognizes that employees, contractors, or third parties with legitimate access may inadvertently or maliciously misuse data. To mitigate the risk, Cloudflare maintains strong controls and provides customers with visibility into user and administrative activity across its services:</p> <ul style="list-style-type: none"> Audit Logs (available in the Cloudflare dashboard and via API) record detailed information about configuration changes, access attempts, and administrative actions. These logs can be exported and integrated with SIEM platforms for centralized monitoring, correlation, and threat detection. Cloudflare Zero Trust (Access and Gateway) provides granular controls over

		<p>user activity, allowing customers to enforce policies that limit data exfiltration.</p> <ul style="list-style-type: none"> • Anomalous activity detection through integrations and customer alerting allows customers to identify unusual login patterns, privilege escalations, and more. • Role-Based Access Control (RBAC) in the Cloudflare dashboard and API allows organizations to assign granular roles and permissions to users.
34	<ul style="list-style-type: none"> • access and activity logging; 	<p>Cloudflare’s measures for logging Security Measures can be found under Annex 2 of the DPA (https://www.cloudflare.com/cloudflare-customer-dpa/) and under the Information Security Exhibit (https://www.cloudflare.com/security-exhibit/), both incorporated in the ToS.</p> <p>Cloudflare provides customers with visibility into system events, configuration changes, and user activity to support compliance, security monitoring, and forensic investigations:</p> <ul style="list-style-type: none"> • Audit Logs captured detailed records of changes made within the Cloudflare dashboard and via API, including who performed the action, what resource was changed, and when the activity occurred. • Logpush enables customers to stream real-time logs directly to supported storage destinations and SIEM platforms. • Cloudflare Zero Trust logs provide insights into user access requests, authentication, and network activity to help customers detect anomalies. • Cloudflare Security Center and Analytics bring together our suite of security products, our security expertise, and unique Internet intelligence as a unified security intelligence solution. • API access logging ensures that API interactions with Cloudflare services are tracked and available for monitoring and reporting.
35	<ul style="list-style-type: none"> • incident detection and response; 	<p>Customers have the option to use their own security tools or Cloudflare’s to enhance detection and monitoring of security events in their environment:</p> <ul style="list-style-type: none"> • Cloudflare Security Center and Analytics bring together our suite of security products, our security expertise, and unique Internet intelligence as a unified security intelligence solution. • Security Event Alerts notify customers in real time of potential threats. • Cloudflare Web Application Firewall (WAF) automatically detects and

		<p>blocks common application vulnerabilities with managed rulesets updated by Cloudflare’s security teams.</p> <ul style="list-style-type: none"> • Cloudflare Bot Management identifies and mitigates malicious automated traffic. • Cloudflare DDoS Protection automatically monitors and mitigates large-scale attacks. • Cloudflare URL Scanner allows customers to examine a site for potential malicious activity. • Cloudflare API Shield includes schema validation and mTLS to detect anomalous API traffic. • Cloudflare SOC and Incident Response operates 24/7 to detect, analyze, and remediate security incidents affecting Cloudflare network and services.
36	<ul style="list-style-type: none"> • loss prevention and recovery; 	<p>Cloudflare will maintain and annually update a comprehensive business continuity framework (“Business Continuity Plan”). This Business Continuity Plan will be tested periodically to ensure that it minimizes the risk of disruption of its obligations under the Agreement. Cloudflare will also maintain and annually update a documented data breach action and response plan.</p> <p>Cloudflare’s IT Security Measures can be found under Annex 2 of the DPA (https://www.cloudflare.com/cloudflare-customer-dpa/) and under the Information Security Exhibit (https://www.cloudflare.com/security-exhibit/), both incorporated in the ToS.</p>
37	<ul style="list-style-type: none"> • data segregation (if using a multi-tenant environment); 	<p>To keep data private and secure, Cloudflare logically isolates each customer's data from that of other customers. Please see section 4.5 in Cloudflare’s Security Exhibit https://www.cloudflare.com/en-gb/security-exhibit/</p>
38	<ul style="list-style-type: none"> • operating system, network, and firewall configuration; 	<p>Our Information Security Exhibit (https://www.cloudflare.com/security-exhibit/) outlines the security measures that Cloudflare maintains to ensure the security, confidentiality, integrity, and availability of Customer data.</p>

		Please see here all the certifications we maintain including those under which we are audited regularly: https://www.cloudflare.com/trust-hub/compliance-resources/
39	<ul style="list-style-type: none"> • staff training; 	Cloudflare will provide security awareness training to Cloudflare employees at the time of hire and annually thereafter. Training will be regularly updated to include applicable information on security topics, including, responsibilities for protecting data and systems, and emerging threats and trends.
40	<ul style="list-style-type: none"> • the ongoing monitoring of the effectiveness of the service provider's controls, including through the exercise of access and audit rights (see Chapter 8); 	<p>Audit reports:</p> <p>Cloudflare maintains multiple security compliance certifications. Customers can download them from the Cloudflare dashboard or make a request with their Cloudflare account team. For more information and to review our public FAQs, please visit our Trust Hub Compliance Resources.</p>
41	<ul style="list-style-type: none"> • policies and procedures to detect activities that may impact firms' information security (eg data breaches, incidents, or misuse of access by third parties) and respond to these incidents appropriately (including appropriate mechanisms for investigation and evidence collection after an incident); and 	Please see row 35 for information about how Cloudflare can support you with incident detection and response.

- procedures for the deletion of firm data from all the locations where the service provider may have stored it following an exit or termination, provided that access to the data by the firm or PRA is no longer required (see Chapters 8 and 10). When deciding when to delete data, firms will need to consider their obligations under data protection law and their potential data retention obligations.

On termination of the contractual relationship, Cloudflare will comply with your instruction to delete Customer Data from Cloudflare systems unless otherwise required by applicable laws.

Cloudflare recognizes individuals’ data protection rights. You have the right to access, correct, update, port, or delete your personal information, and to restrict or object to the processing of your personal information (each of these a “Rights Request”).

When the data retention period expires for a given type of data, we will delete or destroy it. If, for technical reasons, we are unable to do so, we will implement appropriate security measures to prevent any further use of such data.

[Privacy Policy.](#)

Cloudflare provides contractual commitments and technical processes to ensure customer data is securely deleted following a termination of service. Customers must consider their own data retention obligations under applicable law before requesting deletion.

- Under the Cloudflare Data Processing Addendum (DPA), Cloudflare will comply with instructions to remove customer data.
- Certain limited data (e.g., billing records, security logs) may be retained as required by law or for compliance with contractual obligations, after which it is securely deleted.
- Cloudflare will maintain secure data disposal procedures, including but not limited to using secure erase commands, degaussing, and “crypto shredding” as appropriate, and as in accordance with industry standards.

43	<p>7.12 Where data is encrypted, firms should ensure that any encryption keys or other forms of protection are kept secure by the firm or outsourcing provider. The data protected by encryption (although not necessarily the encryption keys themselves) should be provided to the PRA in an accessible format if required, in accordance with Fundamental Rule 7 and other potentially relevant regulatory requirements.</p>	<p>For information on encryption and key management refer to row 31.</p>
44	<p>7.13 The ability of service providers to respond to customer-specific data security requests may vary depending on the service being provided. Generally, the more standardized the service, the more difficult it might be for the service provider to accommodate these requests. The PRA’s focus is on the overall effectiveness of the service provider’s security environment, which should allow firms to meet their regulatory and risk management obligations and be at least as effective as their in-house security environment. As long as service providers can provide assurance that this is the case, the PRA does not have specific expectations around customer-specific requests.</p>	<p>Cloudflare operates a globally standardized security environment across its network and services.</p> <ul style="list-style-type: none"> ● Cloudflare manages the security of the infrastructure and edge network while customers are responsible for defining and implementing the security measures applied to their data, configurations, and applications. ● Customers can tailor their own security posture through controls such as the Web Application Firewall (WAF), DDoS policies, Zero Trust access enforcement, Bot Management, and custom SSL/TLS certificate management. ● Cloudflare maintains multiple security compliance certifications. For more information and to review our public FAQs, please visit our Trust Hub Compliance Resources. ● In addition to third-party tools, customers can leverage Cloudflare services such as Security Insights, Logpush, and Zero Trust dashboards to monitor the security of their data and applications. ● For more information, refer to rows 29 to 43.
<p>8 Access, audit, and information rights</p>		

	Bank and PRA information gathering and investigatory powers	
45	<p>8.1 Independent of the expectations on access, audit, and information rights set out later in this chapter, the Bank and PRA have a range of statutory information-gathering and investigatory powers, some of which may apply directly to outsourced service providers as well as firms. The PRA expects firms to make service providers aware of the powers and requirements as set out in Tables 6 and 7 below, which are not exhaustive. However, failure to do so will not affect their applicability.</p>	<p>Cloudflare acknowledges the resolution authority’s range of statutory information-gathering and investigating powers under applicable law.</p>
	Material outsourcing arrangements	
46	<p>8.3 Building on Chapter 6, the PRA expects firms to take reasonable steps to ensure that written agreements for material outsourcing arrangements provide firms, firms’ auditors, the PRA, the Bank (as a resolution authority), and any other person appointed by firms or the Bank and PRA, with full access and unrestricted rights for audit and information to enable firms to:</p> <ul style="list-style-type: none"> ● comply with their legal and regulatory obligations; and ● monitor the arrangement. 	<p>Cloudflare grants the Customer audit rights as stated under section 5 of the DPA in detail.</p> <p>Cloudflare commits to comply with and maintain the following certifications during the term of the Agreement:</p> <ul style="list-style-type: none"> ● ISO/IEC 27001 (Information Security Management Systems) ● ISO/IEC 27701 (ISO privacy certification) ● ISO/IEC 27018 (Cloud Privacy) ● PCI DSS ● SOC 2 Type II ● C5 Type 2

		<p>Customers can request Cloudflare’s comprehensive yearly audit report which is also available under their dashboard after login.</p> <p>If any necessary information shall be missing or not sufficient to comply with the audit requirements under the Framework the Customer is entitled to conduct an audit. We fully cooperate and we give the resolution authority unrestricted audit and access rights. The scope and other details of any audit are determined in the Agreement.</p>
47	8.4 Access, audit, and information rights in material outsourcing arrangements should include where relevant:	
48	<ul style="list-style-type: none"> data, devices, information, systems, and networks used for providing the outsourced service or monitoring its performance. This may include, where appropriate, the service provider’s policies, processes, and controls on data ethics, data governance, and data security; 	<p>Cloudflare grants audit, access and information rights to Regulated Entities, supervisory authorities and their appointees.</p> <p>Request for an audit needs to be sent on at least thirty (30) days’ written notice to the respective email address. Following receipt of an written audit request, Cloudflare and Customer will discuss and agree in advance on the reasonable start date, scope, duration of, and security and confidentiality controls. Cloudflare may conduct pooled audits and reasonably request Customer to participate in these as long as Customers right to audit is not limited or restricted by the pooled audit procedure.</p> <p>The audit includes the premises and equipment of Cloudflare to ensure they comply with the procedures and working methods stipulated in the Agreement, undertaking to allow access to all Cloudflare relevant facilities, documentation, information and data with restrictions as follows:</p> <p>No access is granted to</p> <p>(i) any data from Cloudflare’s other customers, (ii) Cloudflare’s trade secrets, (iii) any information that could compromise the security of Cloudflare’s systems or premises or cause Cloudflare to breach its obligations under applicable laws or regulations or its security, confidentiality and or privacy obligations to any other Cloudflare</p>

		customer or any third party, (iv) any data or facilities not involved in the Services (as provided to Customer) or not required to show compliance with the Agreement.
49	<ul style="list-style-type: none"> the results of security penetration testing carried out by the outsourced service provider, or on its behalf, on its applications, data, and systems to ‘assess the effectiveness of implemented cyber and internal IT security measures and processes’; 	Cloudflare provides the executive penetration test results summary and gives Customers the possibility to conduct a Penetration test themselves under Cloudflare Customer Penetration Test Policy.
50	<ul style="list-style-type: none"> company and financial information; and 	Cloudflare is a publicly listed company, and therefore its financial statements and other key corporate information are publicly available. Such information is available through Cloudflare Investor Relations Website (https://www.cloudflare.net/home/default.aspx) or via the relevant stock exchange disclosure platform..
51	<ul style="list-style-type: none"> the service provider’s external auditors, personnel, and premises. 	Please see rows 46 and 48.
	Pooled audits and third party certificates and reports	
52	<p>8.7 Firms may use a range of audit and other information gathering methods, including:</p> <ul style="list-style-type: none"> offsite audits, such as certificates and other independent reports supplied by service providers; and onsite audits, either individually or in conjunction with other firms (pooled audits). 	Please see rows 46 and 48.

	Third party certificates and reports	
53	8.9 Certificates and reports supplied by service providers may help firms obtain assurance on the effectiveness of the service provider's controls. (...)	Please see row 46.
	Onsite audits	
54	8.11 Before an onsite audit, the PRA expects firms, individuals, and organisations acting on their behalf to:	
55	<ul style="list-style-type: none"> ● provide reasonable notice to the service provider, unless this is not possible due to a crisis or emergency, or because it would defeat the purpose of the audit. Such notice should include the location and purpose of the visit and the personnel that will participate in the visit; ● verify that whoever is performing the audit has appropriate expertise, qualifications, and skills; and ● take care if undertaking an audit of a multi-tenant environment, (eg a cloud data centre), to avoid or mitigate risks to other clients of the service provider in the course of the audit (eg availability of data, confidentiality, impact on service levels). 	Please see row 48.

56	8.12 Certain types of onsite audit may create an unmanageable risk for the environment of the provider or its other clients, for example, by impacting service levels or the confidentiality, integrity, and availability of data. In such cases, the firm and the service provider may agree alternative ways to provide an equivalent level of assurance, for instance, through the inclusion of specific controls to be tested in a report or certification. The PRA expects that firms should retain their underlying right to conduct an onsite audit. For material outsourcing arrangements, the PRA would expect the firm to inform their supervisor if alternative means of assurance have been agreed.	Please see row 48.
	Pooled audits	
57	8.13 Pooled audits may be organised by groups of firms sharing one or more service providers or facilitated by the service providers. They may be performed by representatives of the participating firms or specialists appointed on their behalf. Pooled audits can be more efficient and cost effective for firms and less disruptive for service providers running multi-tenanted environments. They can also help spread costs and disseminate best industry practices with regard to audit methods among firms.	Please see rows 46 and 48.
9 Sub-outsourcing		

58	<p>9.1 The EBA Outsourcing GL define ‘sub-outsourcing’ as ‘a situation where the service provider under an outsourcing arrangement further transfers an outsourced function to another service provider’, which may also include part of an outsourced function. The PRA Rulebook also explicitly acknowledges that a service provider may perform ‘a process, a service or an activity which would otherwise be undertaken by the firm itself [...] directly or by sub-outsourcing’.</p> <p>Sub-outsourcing, which is also sometimes referred to as ‘chain’ outsourcing, can amplify certain risks in material outsourcing, including:</p> <ul style="list-style-type: none"> • limiting firms’ ability to manage the risks of the outsourcing arrangement, in particular, where there are large chains of sub-outsourced service providers spread across multiple jurisdictions; and • giving rise to additional or increased dependencies on certain service providers, which the firm may be fully aware of or may not want. 	<p>Subcontractors:</p> <p>Cloudflare recognizes that Regulated Entities need to consider the risks associated with subcontracting. To ensure Regulated Entities retain oversight of any subcontracting supporting critical or important functions, Cloudflare will comply with clear conditions designed to provide transparency and choice.</p> <p>In particular, Cloudflare will:</p> <p>Provide a list of the critical subcontractors under the dashboard</p> <ul style="list-style-type: none"> • provide any requested necessary information about our subcontractors; • provide advance notice of material changes to our critical subcontractors with an objection right; and • give Regulated Entities the ability to terminate in specific circumstances under material changes on subcontracting arrangements in line with the Framework. <p>Subprocessors:</p> <p>Under section 4.4 of the DPA the reference to the website where a detailed list of all sub Processors is accessible is contained (https://www.cloudflare.com/gdpr/subprocessors/) and also the procedure in case of changes.</p>
	Firms’ oversight of sub-outsourcing	
59	<p>9.3 The PRA expects firms to assess the relevant risks of sub-outsourcing before they enter into an outsourcing agreement. It is important that firms have visibility of the supply chain, and that service providers are encouraged to</p>	<p>Cloudflare will provide all the information required in the outsourcing register for each of our subcontractors. Please see row 58.</p>

		facilitate this by maintaining up-to-date lists of their sub-outsourced service providers.	
60	9.4	The PRA expects firms to pay particular attention to the potential impact of large, complex sub-outsourcing chains on their operational resilience, including their ability to remain within impact tolerances during operational disruption. Firms should also consider whether extensive sub-outsourcing could compromise their ability to oversee and monitor an outsourcing arrangement.	Please see row 58.
61	9.5	Firms should assess whether sub-outsourcing meets the materiality criteria set out in Chapter 5, which includes the potential impact on the firm's operational resilience and the provision of important business services. (...)	Please see row 58.
62	9.6	Firms should ensure that the service provider has the ability and capacity on an ongoing basis to appropriately oversee any material sub-outsourcing in line with the firm's relevant policy or policies. This includes establishing that the service provider has in place robust testing, monitoring, and control over its sub-outsourcing.	<ul style="list-style-type: none"> ● Cloudflare maintains a Third Party Risk Management Policy that establishes security requirements for suppliers based on the data exchanged and the criticality of the vendor. ● The program covers third party risk, compliance, and performance management, with performance measured by the team owning the vendor relationship and security evaluations conducted by the Security team. ● Vendors are required to complete questionnaires and provide assurance documentation, including policies, certifications, and applicable security certifications (such as ISO or SOC 2). Vendors without these certifications must share compensating controls. ● Cloudflare's Third Party Code of Conduct is formulated for suppliers, resellers, and partners, with rigorous screening, vetting, routine monitoring, and auditing at onboarding and over time. ● High risk vendors are reviewed prior to onboarding and annually thereafter.

63	<p>9.7 If the proposed material sub-outsourcing could have significant adverse effects on a material outsourcing arrangement or would lead to a substantive increase of risk, the firm should exercise its right to object to the material sub-outsourcing and/or terminate the contract.</p>	<p>Please see row 58. Cloudflare grants an objection right as well as a termination right in case of material changes that lead to increase of risk and non-compliance with regulatory provisions.</p>
	<p>Written agreement</p>	
64	<p>9.9 In line with Chapter 6, the PRA expects written agreements for material outsourcing to indicate whether or not material sub-outsourcing is permitted, and if so:</p> <ul style="list-style-type: none"> ● specify any activities that cannot be sub-outsourced; ● establish the conditions to be complied with in the case of permissible ● sub-outsourcing, including specifying that the service provider is obliged to oversee those services that it has sub-contracted to ensure that all contractual obligations between the service provider and the firm are continuously met; ● require the service provider to: <p>obtain prior specific or general written authorisation from the firm before transferring data (see Article 28 GDPR); and</p> <p>inform the firm of any planned sub-outsourcing or material changes, in particular where that might affect the ability of the service provider to</p>	<p>Please see row 58.</p>

	<p>meet its responsibilities under the outsourcing agreement. This includes planned significant changes to sub-contractors and to the notification period. Firms should be informed sufficiently early to allow them to at least carry out a risk assessment of the proposed changes and object to them before they come into effect;</p> <ul style="list-style-type: none"> ensure that, where appropriate, firms have the right to: <p>explicitly approve or object to the intended material sub-outsourcing or significant changes thereto; and</p> 	
10 Business continuity and exit plans		
65	<p>10.1 For each material outsourcing arrangement, the PRA expects firms to develop, maintain, and test a:</p>	<p>Cloudflare recognizes the importance of business continuity and exit planning. We do our own continuity planning for our services. You can also use our services in your own business continuity and exit planning.</p>
66	<ul style="list-style-type: none"> business continuity plan; and 	<p>Cloudflare will maintain and annually update a comprehensive business continuity framework (“Business Continuity Plan”). This Business Continuity Plan will be tested periodically to ensure that it minimizes the risk of disruption of its obligations under the Agreement. Cloudflare will also maintain and annually update a documented data breach action and response plan.</p> <p>Cloudflare’s IT Security Measures can be found under Annex 2 of the DPA (https://www.cloudflare.com/cloudflare-customer-dpa/) and under the Information Security Exhibit (https://www.cloudflare.com/security-exhibit/), both incorporated in the ToS.</p>

67	<ul style="list-style-type: none"> documented exit strategy, which should cover and differentiate between situations where a firm exits an outsourcing agreement: in stressed circumstances, (eg following the failure or insolvency of the service provider (stressed exit)); and through a planned and managed exit due to commercial, performance, or strategic reasons (non-stressed exit). 	<p>Cloudflare recognizes that Regulated Entities need to be able to exit our Services without undue disruption to their business and without limiting their compliance with statutory requirements. Therefore, Cloudflare offers to continue to provide the services under the agreement for a pre-defined period of time after expiration or termination of the Agreement to Regulated Entities (“Transition Period”) upon request.</p>
	<p>Business continuity</p>	
68	<p>10.3 Firms should implement and require service providers in material outsourcing arrangements to implement appropriate business continuity plans to anticipate, withstand, respond to, and recover from severe but plausible operational disruption.</p>	<p>Please see row 66.</p>
69	<p>10.4 An important objective of the access, audit, and information rights in Chapter 8 is to enable firms, the PRA, and the Bank to assess the effectiveness of service providers’ business continuity plans. In particular, they should be able to assess the extent to which they may enable the delivery of important business services for which a firm relies (wholly or in part) on the service provider, within the firm’s impact tolerance in severe but plausible scenarios</p>	<p>For information on the access, audit and information rights please see section 8.</p>

70	<p>10.5 In material cloud outsourcing arrangements, the PRA expects firms to assess the resilience requirements of the service and data that are being outsourced and, with a risk-based approach, decide on one or more available cloud resiliency options, which may include: multiple data centres spread across geographical regions; multiple active data centres in different availability zones within the same region, which allows the service provider to re-route services if a data centre goes down; a hybrid cloud (ie a combination of on-premises and public cloud data centres); multiple or back-up vendors; retaining the ability to bring data or applications back on-premises; and/or any other viable approach that can achieve and promote an appropriate level of resiliency.</p>	<p>Cloudflare runs an anycast network to ensure a fast and reliable service. Details can be found here: https://www.cloudflare.com/learning/cdn/glossary/anycast-network/ and here: https://blog.cloudflare.com/cloudflares-architecture-eliminating-single-p/</p> <p>Cloudflare enables the Customer to access and export its data throughout the duration of the contract. Customer can access their logs through the dashboard after login and can use Logpush to save the data for as long as they want in their respective storage that they control.</p>
	<p>Stressed exits</p>	
71	<p>10.10 Firms' exit plans should cover stressed exits and be appropriately documented and tested as far as possible.</p>	<p>Cloudflare recognizes that Regulated Entities need to be able to exit our Services without undue disruption to their business and without limiting their compliance with regulatory requirements. Therefore Cloudflare offers to continue to provide the services under the agreement for a pre-defined period of time after expiration or termination of the Agreement to Regulated Entities ("Transition Period") upon request.</p> <p>We also provide further necessary assistance with our Technical Support that can be purchased. Please see here: https://developers.cloudflare.com/support/contacting-cloudflare-support/</p> <p>Furthermore Cloudflare enables the Customer to access and export its data throughout the duration of the contract. Customer can access their logs through</p>

		the dashboard after login and can use Logpush to save the data for as long as they want in their respective storage that they control.
72	10.11 A key objective of the stressed exit part of exit plans is to provide a last resort risk mitigation strategy in the event of disruption that cannot be managed through other business continuity measures, including those mentioned in the previous section, (eg the insolvency or liquidation of a service provider).46	