

Foresight - Terms & Conditions

(G-Cloud 15)

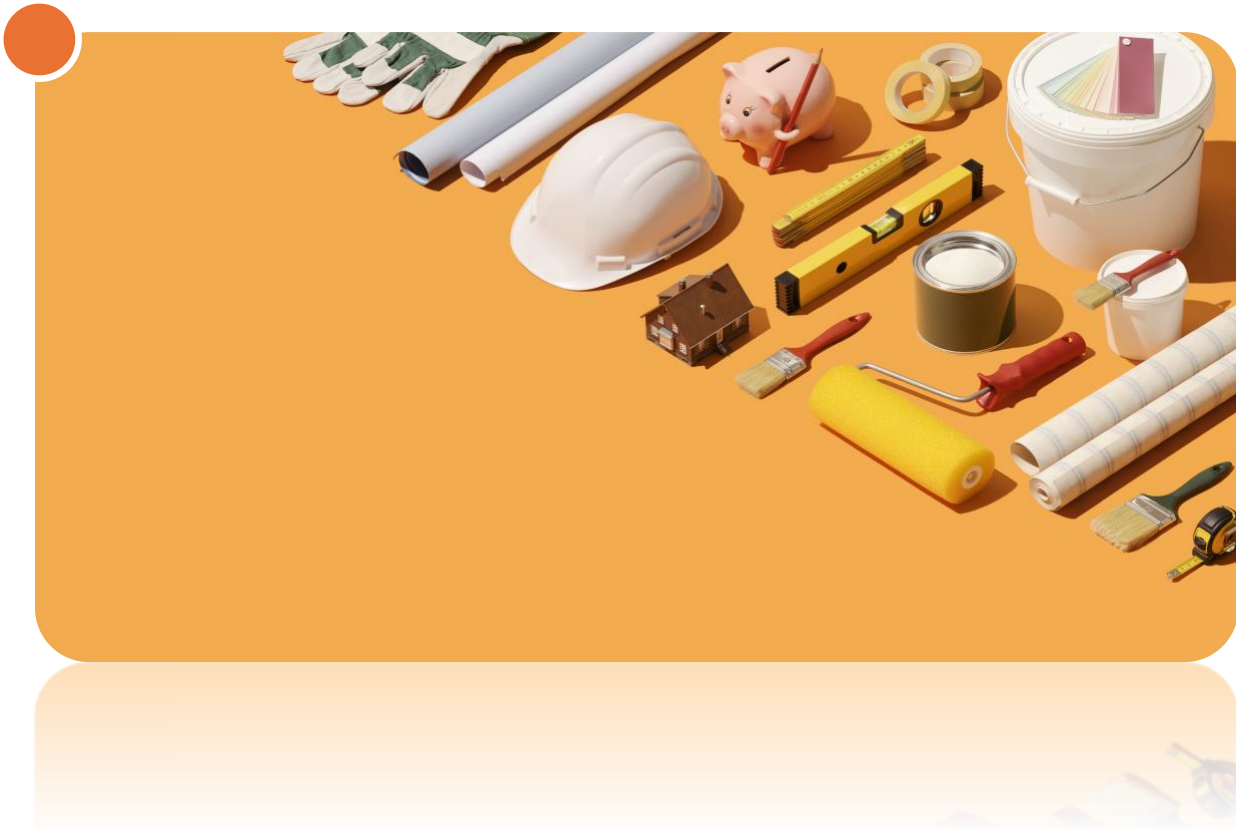


Table of Contents

1. Definitions and interpretation	3
2. Ordering and provisioning	3
3. Customer responsibilities	3
4. Charges and payment.....	3
5. Service levels, maintenance and credits	4
6. Security.....	4
7. Data protection	4
8. Business continuity and disaster recovery.....	5
9. Intellectual property and licences	5
10. Warranties.....	5
11. Indemnities	5
12. Liability.....	6
13. Audit and records	6
14. Change control.....	6
15. Suspension.....	6
16. Term and termination	6
17. Confidentiality and FOIA	6
18. Ethics and compliance	7
19. Notices.....	7
20. Governing law and jurisdiction.....	7
Schedule A — Data Processing Annex (summary).....	7

These Supplier Terms apply to Call-Off Contracts awarded via G-Cloud 15 and must be read with the CCS Framework and Call-Off Terms. If there is any conflict, the Call-Off Terms take precedence. One set of Supplier Terms applies to all Buyers.

1. Definitions and interpretation

Capitalised terms have the meanings in the G-Cloud 14 Framework and Call-Off Terms unless defined here. In these Terms, “Service” means the Foresight SaaS described in the Service Definition; “Customer Data” means data submitted by or on behalf of the Customer; “Authorised Users” means users permitted by the Customer to access the Service. References to legislation include amendments and replacements.

2. Ordering and provisioning

- *Scope. The Service covers Cloud Software (Lot 2b) and any Cloud Support (Lot 3) expressly stated on the Order Form.*
- *Provisioning. Supplier provides a secure, multi-tenant SaaS environment; the Customer configures users, roles and access.*
- *Commencement. Access is enabled following Contract signature and receipt of any initial information reasonably required (e.g., IdP metadata).*

3. Customer responsibilities

- *Access control. Maintain accurate user lists and allocate appropriate roles. Notify Supplier promptly of leavers/changes.*
- *Acceptable use. Do not introduce malware, disrupt the Service, attempt unauthorised access, or infringe IP or privacy rights.*
- *Data accuracy. Ensure Customer Data, including schedules and metadata, is accurate and lawful to process.*

4. Charges and payment

- *Charges. As per the published G-Cloud Pricing and/or the Order Form, exclusive of VAT.*
- *Invoicing. Invoices are issued annually or monthly in arrears unless otherwise agreed.*
- *Payment. Payable within 30 days of invoice date. Late payment interest may be charged in accordance with the Call-Off Terms.*
- *Indexation. Unless stated otherwise, prices are fixed for the Initial Term. Any indexation thereafter will be at most CPI (UK) once per renewal year.*

5. Service levels, maintenance and credits

Availability target is 99.5% measured monthly, excluding planned maintenance and circumstances in the Call-Off relief events. Support hours, response and resolution objectives are defined in the Service Definition. Planned maintenance windows will be notified reasonably in advance. Emergency security maintenance may occur out of hours with short notice where necessary.

Severity	Illustrative examples	Target response	Target resolution (objective)
Sev 1 — Critical outage	Platform unavailable; data loss risk	1 hour	Same business day
Sev 2 — Major degradation	Material feature impairment for many users	2 hours	1 business day
Sev 3 — Minor impact	Workaround available; limited scope	1 business day	5 business days
Sev 4 — Requests/How-to Questions, requests, minor changes		2 business days	As scheduled

Service credits (if expressly stated on the Order Form) will be the sole financial remedy for availability shortfalls. Credits are not payable where the Customer is in material breach or where an exclusion applies.

6. Security

- *Controls.* Supplier maintains ISO/IEC 27001:2013 and Cyber Essentials Plus.
- *Hosting.* Primary hosting is in AWS London (eu-west-2).
- *Encryption.* TLS 1.2+ in transit; AES-256 at rest with AWS KMS-managed keys.
- *Perimeter and monitoring.* Cloudflare WAF, network segmentation, intrusion detection, logging and audit.
- *Identity.* SSO (SAML/OIDC), enforced MFA for admin, RBAC based on least-privilege.
- *Testing.* Regular third-party penetration testing, including AI components where applicable.

7. Data protection

- *Roles.* The Customer acts as Controller and the Supplier as Processor for Customer Data processed in the Service.
- *Processing details.* Subject-matter: provision of the Service; Duration: Contract term plus any agreed retention; Nature/Purpose: hosting, processing and analytics of project schedules and user identities; Categories: names, business emails, usernames, roles, and schedule resource identifiers; Data subjects: Customer personnel and authorised users.

- *Sub-processors. Supplier uses sub-processors under written contracts with at least equivalent protections and will notify changes with a right to object. A current list is available on request.*
- *International transfers. Data residency is UK by default. Any international transfer will use adequacy or appropriate safeguards (e.g., IDTA or SCCs).*
- *DPO. Contact: dpo@foresight.works.*
- *Security incidents. Supplier will notify without undue delay upon becoming aware of a personal data breach affecting the Service, providing information to support the Customer's obligations.*
- *Exit and deletion. On exit, Supplier will provide a complete export on request and securely delete residual copies following Customer confirmation, subject to any legal retention obligations.*

8. Business continuity and disaster recovery

- *Backups. Encrypted backups are taken and restore procedures are tested periodically.*
- *Targets. Indicative objectives are RTO: [insert] and RPO: [insert].*
- *Resilience. Multi-AZ cloud architecture with documented incident response runbooks.*

9. Intellectual property and licences

- *Ownership. Supplier (or its licensors) owns all IPR in the Service and documentation. Customer Data remains Customer property.*
- *Licence. The Customer receives a non-exclusive, non-transferable right for Authorised Users to access and use the Service for internal purposes during the term.*
- *Open-source. Supplier manages open-source components in accordance with their licences and maintains a register on request.*
- *Feedback. Supplier may use feedback to improve the Service; no obligation to implement.*

10. Warranties

- *Conformance. The Service will materially conform to the Service Definition.*
- *Support. Support will be provided with reasonable skill and care by appropriately skilled personnel.*
- *Compliance. Supplier will comply with applicable laws, including data protection and information security obligations.*

11. Indemnities

- *IPR. Supplier will defend and indemnify the Customer against third-party claims that the Service infringes UK IPR, subject to customary conditions and exclusions.*

- *Data protection. Each party will indemnify the other for fines or claims caused by its breach of data protection law, to the extent permitted by the Call-Off Terms.*

12. Liability

Nothing limits or excludes liability for death or personal injury caused by negligence, fraud or fraudulent misrepresentation, or any liability which cannot lawfully be limited. Subject to the foregoing, each party's aggregate liability in any Contract Year is capped at 100% of the Charges paid or payable in that Contract Year. Neither party is liable for indirect or consequential loss, or loss of profit, revenue, or goodwill.

13. Audit and records

- *Records. Supplier will maintain records sufficient to demonstrate compliance with these Terms and the Call-Off.*
- *Audit. Subject to reasonable notice and confidentiality, the Customer or its auditor may audit compliance during business hours no more than once per year, unless required by law or following a material incident.*

14. Change control

Material changes to the Service will be communicated in advance with reasonable notice. Functional changes that adversely affect the Customer's ability to meet business requirements will be addressed via configuration, guidance or reasonable workarounds.

15. Suspension

Supplier may suspend access where necessary to address security risks, to comply with law, or for material breach by the Customer, and will restore access promptly once the issue is resolved.

16. Term and termination

- *Term. As per the Order Form and Call-Off Terms, with any permitted renewals.*
- *Termination for cause. Either party may terminate for material breach not remedied within 30 days of notice, or for insolvency.*
- *Effect of termination. Access ceases; Supplier provides export and performs secure deletion per Clause 7.*

17. Confidentiality and FOIA

- *Confidentiality. Each party will protect the other's Confidential Information and use it only for the Contract.*
- *FOIA. Supplier will reasonably assist the Customer to respond to information requests; disclosure decisions remain with the Customer.*

18. Ethics and compliance

- *Anti-bribery. Each party will comply with the Bribery Act 2010 and maintain adequate procedures.*
- *Modern Slavery. Each party will comply with the Modern Slavery Act 2015 policies and reporting.*
- *Equality. Each party will comply with applicable equality and diversity legislation.*
- *Export control and sanctions. Each party will comply with applicable export control and sanctions laws.*

19. Notices

Formal notices must be in writing and sent to the addresses set out in the Order Form, with a copy to legal@foresight.works for the Supplier. Notices by email are effective on the next business day after sending.

20. Governing law and jurisdiction

These Terms and any non-contractual obligations are governed by the laws of England and Wales. The courts of England and Wales have exclusive jurisdiction.

Schedule A — Data Processing Annex (summary)

Item	Details
Controller/Processor	<i>Customer as Controller; Supplier as Processor for Customer Data within the Service.</i>
Subject-matter & duration	<i>Provision of the Service for the Contract term and any agreed retention.</i>
Nature & purpose	<i>Hosting, processing and analytics of project schedules and user identities to deliver insights and reporting.</i>
Categories of data	<i>First/last name, business email, username, role; schedule resource identifiers (e.g., resource names/codes).</i>
Data subjects	<i>Authorised users and Customer personnel.</i>
Location & transfers	<i>UK (AWS London, eu-west-2) by default. Transfers only with adequacy or safeguards.</i>
Security measures	<i>TLS 1.2+ in transit; AES-256/KMS at rest; SSO; MFA for admin; RBAC; logging and monitoring; regular testing.</i>
Return/Deletion on exit	<i>Complete export available; secure deletion of residual copies after Customer confirmation.</i>
DPO	<i>dpo@foresight.works</i>

