

DORA Statement on Contractual Compliance – FundApps Limited

1. Overview

- 1.1 FundApps Limited ("**FundApps**") takes compliance seriously and we are dedicated to supporting our customers' compliance with regulatory obligations. Compliance is at the heart of everything we do.
- 1.2 For financial entities who are subject to the EU's Digital Operational Resilience Act ("**DORA**"), we offer a DORA Addendum to facilitate their compliance with mandatory contractual requirements and other measures that they need to ensure that they have in place with FundApps.
- 1.3 This DORA Statement on Contractual Compliance ("**Statement**") is designed to assist financial entities track DORA requirements to the FundApps DORA Addendum (the "**Addendum**"). It aligns clauses from the Addendum and explains how the Addendum is designed to meet financial entity requirements.
- 1.4 In preparing the Addendum and this Statement, we have sought to provide you with an easy-to-use set of tools to enable you to validate that your engagement with us meets the required standards under DORA. This Statement should be read alongside the [FundApps Operational Resilience Statement](#), which sets out more detail on how FundApps' information security and business continuity measures align to financial entity requirements under DORA and its related Regulatory Technical Standards.
- 1.5 The minimum mandatory contractual terms are specified in Articles 28 and 30 of DORA, with additional terms required to be included in circumstances where financial entities determine that the "ICT services" being provided by their "ICT third-party service providers" support their "critical or important functions" (each as defined under DORA).
- 1.6 FundApps provides its compliance solutions by virtue of a Software-as-a-Service offering. FundApps therefore accepts that its services involve 'ICT services' within the meaning of DORA. FundApps' view is that its ICT services do not support critical or important functions of its financial entity customers, but FundApps recognises that financial entities may make different assessments depending on what FundApps solutions they use and how they use them.
- 1.7 We have taken into account financial entity obligations under DORA, while at the same time, taking a proportionate approach (as contemplated under DORA) to contractualising risk, to ensure that we can continue to provide you with a service that represents good value for money and which is in keeping with our standard operating model.
- 1.8 FundApps' Addendum therefore supports mandatory contractual terms for ICT services generally as well as contractual terms for ICT services supporting critical or important functions, where a financial entity has made that assessment. In this Statement, the following colour-coding has been applied to differentiate between two key categories of contractual provisions:

Colour Code	Category of ICT service provision
	Provisions for inclusion in all impacted arrangements
	Provisions for inclusion only in arrangements for the supply of ICT services which support the financial entity's critical or important functions

- 1.9 If a financial entity has made a determination that it uses or will use FundApps' services (or a part thereof) to support a critical or important function of the financial entity, then both Parts 1 and 2 of the Addendum apply, and all aspects of this Statement are relevant. If, however, a financial entity has not determined that it uses or will use FundApps' services (or a part thereof) to support any of its critical or important functions, then only Part 1 of the Addendum will apply.
- 1.10 If you have any queries regarding this Statement or the Addendum, please contact legal@fundapps.co.

DORA Reference	Subject Matter	Addendum Ref.	Compliance Approach
Article 28 – General Principles			
Article 28(5)	Information Security Standards	Clause 6.1	<p>We recognise that financial entities are required to ensure that the ICT third-party service providers with whom they contract comply with "appropriate information security standards" and, in some cases, "the most up-to-date and highest quality information security standards".</p> <p>We commit in the Addendum to implement and maintain appropriate information security standards. Moreover, we have in place certifications to internationally recognised standards like ISO27001 and SOC2, and we also commit to maintain certification to those standards in the Addendum.</p> <p>In order to see how we support financial entities with their own operational resilience compliance, we have also set out Operational Resilience Compliance Statement (which is a broader overview of the operational resilience measures which we have in place to meet financial entity requirements under DORA and the Implementing Regulations), and we are able to contractually commit to having in place and maintaining certification to ISO27001 and SOC 2 standards.</p>
Article 28(6)	Audit and Inspections	Clause 17	<p>Article 28(6) requires the financial entity to:</p> <ul style="list-style-type: none"> pre-determine the frequency of audits and inspections as well as the areas to be audited; adhere to commonly accepted audit standards in line with any supervisory instruction on the use and incorporation of such audit standards; where contractual arrangements entail high technical complexity, verify that auditors, whether internal or external, or a pool of auditors, possess appropriate skills and knowledge to effectively perform the relevant audits and assessments. <p>To accommodate these requirements, we have included the following provisions in clause 17 of the Addendum:</p> <ul style="list-style-type: none"> The scope of the right is limited to reviewing our performance of the Services and compliance with the Agreement generally; 30 days' notice must be provided (save for in certain limited circumstances); A requirement, where a third party is engaged, to verify that the third party and its personnel have the necessary skills, knowledge and experience to exercise the right; A requirement to exercise the right during standard business hours (unless this is not possible) and no more than once per any 12-month period (unless a more frequent exercise is required by a regulator), with each exercise being for a maximum of 1 business day (unless a longer period is required by a regulator); and A requirement to exercise the right in a risk-based and proportional manner, taking into account the legal requirements, the context and the nature of the Service. <p>We consider these to be reasonable and proportionate restrictions on an otherwise broad right to conduct inspections and audits.</p> <p>We also note that FundApps is subject to a number of independent audits and inspections in the ordinary course, and as part of maintaining its certifications. FundApps requires that, in advance of exercising any audit right, you should first consider whether our existing audit reports, third party certifications are sufficient and other documentary evidence is sufficient. Financial entities may take these into account in their due diligence processes for selecting and assessing ICT third party service providers and should have in place a policy for contracting with ICT third party service providers which determines where the financial entity can rely on other information for the purposes of assurance, without undertaking its own audit.</p> <p>See also our comments alongside the requirement under Article 30(3)(e) which covers rights of audit.</p>
Article 28(7)	Termination	Clause 11	<p>We have included additional termination rights in clause 11 of the Addendum, the wording of which is closely aligned with the wording in Article 28(7) of DORA.</p> <p>Where those termination rights are based on a subjective standard (e.g. "circumstances deemed capable of altering the performance of the functions", or "evidenced weaknesses pertaining to risk management"), we have asked that you are able to "reasonably demonstrate" that the relevant circumstances have occurred. We consider this to be a reasonable position, and in line with market norms for termination rights which hinge on the existence of certain facts or circumstances.</p>
(a)	Termination	Clause 11.1(a)	<p>To avoid a situation where those termination rights have to be exercised immediately (where termination would not be the preferred outcome for either party), we have built in a requirement to provide written notice of any circumstances which would otherwise give rise to the termination right, with sufficient detail to allow us at least 30 days to remedy the circumstances before the termination rights are exercised. Again, this is in keeping with typical approaches to termination rights, where the other party would be offered an ability to remedy the circumstance giving rise to the termination trigger in the first instance. (We note that DORA does not require the termination rights to be exercisable immediately – and as such, this is in keeping with the requirements of the Regulation).</p> <p>We also note that a number of these termination rights would arise in circumstances where we are not otherwise in breach of our obligations under the Agreement in place between us. In those circumstances, we consider it reasonable that we should not be required to refund any fees paid in advance, and further that you should not have an ability to bring a claim for breach of contract or otherwise against us in connection with the Agreement.</p>
(b)	Termination	Clause 11.1(b)	
(c)	Termination	Clause 11.1(c)	
(d)	Termination	Clause 11.1(d)	
Article 28(8)	Exit	Clause 18	<p>This Article requires a financial entity to:</p> <ul style="list-style-type: none"> put in place exit strategies, which take into account certain risks; ensure that they are able to exit contractual arrangements without disruption to their business activities, limiting compliance with their regulatory requirements, and/or detriment to the continuity and quality of services provided to their clients;

DORA Reference	Subject Matter	Addendum Ref.	Compliance Approach
			<ul style="list-style-type: none"> have in place exit plans, which are documented and sufficiently tested and reviewed; and identify alternative solutions / develop transition plans. <p>We believe that inclusion of a contractual obligation regarding the provision of transitional assistance, as contemplated under Article 30(3)(f) of DORA, is sufficient to enable you to satisfy this requirement from a contractual perspective. You will need to put in place measures in the background to ensure that, for example, you can quickly engage a replacement supplier in the event that this Agreement is terminated / expires.</p> <p>We are amenable to providing additional support and assistance to you during any transition period (including e.g. with respect to your exit plan), on the basis that such support and assistance (including the applicable fees) will be agreed between us in a separate order form or similar document.</p> <p>FundApps already offers a commitment to provide Client Data to the Client on request in a readable format and in accordance with the terms of the Agreement.</p> <p>See also our comments alongside the requirement under Article 30(3)(f).</p>
Article 30 – Key Contractual Provisions			
Article 30(1)	General	N/A	<p>Whilst DORA requires that the full contract in place between the financial entity and the ICT third-party service provider is set out in "one written document", there is no prohibition on incorporating documents into that written contract by reference provided that those are made available to the parties in a downloadable, durable and accessible format. All contractual documents are in writing and are incorporated into the one agreement.</p> <p>For the most part, we have sought to include all relevant terms (including service levels) within the body of the Agreement in place between us. Your Order Form is the main contractual document issued to you (incorporating a link to the contract terms on the signature page), and as such forms part of the overall agreement. The core terms themselves are located on our policy hub (General Terms), where the PDF version of the terms can be downloaded.</p> <p>Where there are exceptions (e.g. our Operational Resilience Compliance Statement, our IS policies and service documentation, which are available (via our policy hub), we will make those available to you in a form which you can readily access and download.</p>
Article 30(2)			
(a)	Service Description	Clause 4.1	<p>We have incorporated a description of the Services into the Addendum by reference.</p> <p>This reflects our standard approach to describing the services which we provide. Our Order Form lists the services clients subscribe to - we otherwise link to our "service documentation" (https://docs.fundapps.co/) within the Agreement, which outlines what the service/products comprise in more detail.</p>
	Subcontracting	Clauses 4.2 and 4.3 Clause 16	<p>We engage certain subcontractors to provide aspects of the Services, and it is possible that the subcontracted aspects of the Services may support your critical or important functions (or parts thereof).</p> <p>A list of those subcontractors as at the Effective Date is available [here – https://policies.fundapps.co/fundapps-policy-portal/-LrODnq5HI65-TLW7fbC/legal-information/dora/subcontractors-and-service-location], and that list is incorporated by reference via clause 4.2 of the Addendum.</p> <p>We are able to commit to remaining responsible for all acts and omissions of our subcontractors in respect of the sub-contracted services.</p> <p>We have also included a number of additional controls / conditions in respect of our subcontracting in clause 16 of the Addendum, in particular to assist you with satisfying your need to manage ICT third-party risk through our supply chain. These include:</p> <ul style="list-style-type: none"> A commitment to monitor the subcontractors to ensure that our contractual obligations to you are continuously met; To put in place a written agreement with the subcontractors which contains certain minimum protections (including whether regards to service levels, information security, and rights of access, inspection and audit); and To notify of any material changes to our subcontracting arrangements (with a right for you to object to any such changes and to ultimately terminate the arrangement if your objection is not resolved). <p>Aside from the protections we have included in clause 16 of the Addendum, we are not in a position to further fetter our ability to engage subcontractors to provide elements of the services, nor to flow additional terms down through our supply chain (particularly with regards to our existing subcontractors and those providing one-to-many services to us).</p> <p>We note that financial entities are required to be "proportionate" when assessing the conditions to be applied in respect of subcontracting; we believe that the controls we have included in the Addendum reflect a proportionate position in light of the nature of our services and how we expect those to be used within your business.</p> <p>We also note that we have provided robust guarantees regarding the locations from which we will provide our services and from where Client Data is to be processed / stored, in addition to compliance with appropriate information security standards. Those should provide you with comfort regarding the approach we are taking towards service provision and risk management generally.</p>

DORA Reference	Subject Matter	Addendum Ref.	Compliance Approach
(b)	Location of Service	Clause 5.1	<p>The locations from where the Services are to be provided and where the Client Data is to be processed, including the storage location, are set out [here - https://policies.fundapps.co/fundapps-policy-portal/-LrODnq5HI65-TLW7fbC/legal-information/dora/subcontractors-and-service-location].</p> <p>As required under DORA, we can contractually commit to notifying you in advance of any changes to the service locations.</p> <p>We are not able to agree to any further conditions or restrictions on our use of particular service locations and note that such additional restrictions are not mandated under DORA.</p>
(c)	Information Security Standards	Clause 6.1	<p>We have included a commitment to "implement and maintain appropriate information security standards to ensure availability, authenticity, integrity and confidentiality of the Client Data".</p> <p>Client Data is to have the same meaning as given to it in the underlying agreement in place between us - but we believe this captures the categories of data (including personal data) which are required to be protected pursuant to DORA.</p> <p>For further information on our information security measures, please refer to our IS policies (https://policies.fundapps.co/fundapps-policy-portal/-LrODnq5HI65-TLW7fbC/fundapps-policies/information-security-management-system), which we agree to adhere to contractually. Furthermore, please refer to Clause 8 of our general terms for our general approach to confidentiality, and Schedule C for data protection provisions.</p> <p>See also our comments alongside the Article 28(5) requirements.</p>
(d)	Recovery of Data	Clause 7	<p>Clause 7 of the Addendum details the approach we are able to take with regards to ensuring access, recovery and return of data in the event of our insolvency, resolution or discontinuation of our business, or in the event of the termination of the contractual arrangements.</p> <p>Broadly, in the event that the Agreement terminates or expires, or on the insolvency, resolution or discontinuation of our business operations, we shall provide Client Data to you on request in a readable format. We are happy to do this free of charge.</p> <p>The approach specified is aligned with our general approach to the return of data as set out in our agreement with you.</p> <p>We note that DORA simply requires that such provisions exist in the contractual arrangement – and is not prescriptive regarding their substance (other than to require that the data is returned in an "easily accessible format").</p>
(e)	Service Levels	Clause 8.1	<p>We are able to commit to providing the Services so as to meet the "Agreed Service Levels", which are the service levels set out in the Agreement in place between us (see for example Schedules A and B of our general terms: https://policies.fundapps.co/fundapps-policy-portal/-LrODnq5HI65-TLW7fbC/legal-information/general-terms).</p> <p>Unless we have agreed something else with you, we do not update our service levels during the term of our engagement – they will remain contractually the same for all of our clients.</p>
(f)	Incident Management	Clause 9	<p>We have included an obligation reflective of the requirement of DORA, to provide such assistance as you may reasonably require where an ICT incident occurs that is related to the Services.</p> <p>We would expect you to act reasonably in determining whether you require such assistance.</p> <p>As contemplated under DORA, we would need to charge additional sums for provision of this assistance and have determined those costs <i>ex ante</i> on the basis of a rate of £200 per hour.</p>
(g)	Cooperation with Regulators	Clause 10	<p>We have included a commitment to cooperate fully with Regulators (including competent authorities / resolution authorities) and persons appointed by them in the course of such Regulators performing their regulatory functions in relation to the Service.</p> <p>We would expect you to notify us if you receive inquiries from a Regulator which relate to the Services.</p> <p>As is permitted under DORA, we would need to charge additional sums for provision of this assistance and have determined those costs <i>ex ante</i> on the basis of a rate of £200 per hour unless otherwise agreed in writing.</p>
(h)	Termination	Clause 11.1(e)	<p>We have included an ability for you to terminate the Agreement where required to do so by a Regulator. That right is to be exercised by the provision of written notice to us but would not be subject to the same 30-day cure period as exercise of your other termination rights under the Addendum.</p> <p>Per our comments on Article 28(7), where the Regulatory decision is not based on a breach by us of our obligations, we would not expect to refund any fees paid in advance, and you would not have any further ability to bring a claim for breach of contract or otherwise against us in connection with the Agreement.</p> <p>See also our comments alongside the Article 28(7) requirements.</p>

DORA Reference	Subject Matter	Addendum Ref.	Compliance Approach
(i)	Participation in Client Training Programmes	Clause 12	<p>Under DORA, it is open to you to determine whether or not it is "appropriate" to include us in your security awareness programmes and operational resilience training.</p> <p>If you would like to include us, we would be open to participating subject to the agreement of applicable terms (including as to fees). The condition applicable to our participation can be more appropriately documented in those terms (since those will likely vary on a case-by-case basis).</p>
Article 30(3)			
(a)	Service Levels and Reporting	Clause 8.1 Clause 13	<p>The Agreement in place between us will set out the "Agreed Service Levels" (see Schedules A and B of our terms: https://policies.fundapps.co/fundapps-policy-portal/-LrODnq5HI65-TLW7fbC/legal-information/general-terms). Those feature full descriptions of the service levels and comprise precise performance targets to allow you to effectively monitor our provision of the Services (including response and remediation times for technical errors).</p> <p>Unless we have agreed something else with you, we do not update our service levels during the term of our engagement – they will remain contractually the same for all of our clients.</p> <p>The Agreement also sets out our reporting obligations in relation to any failure to meet the Service Levels.</p> <p>See also our comments alongside the Article 30(2)(e) requirements.</p>
(b)	Reporting	Clause 13	<p>The Agreement in place between us sets out our reporting obligations and notice periods for such reporting, including what reports need to be provided in relation to any failure to meet the Agreed Service Levels.</p> <p>We will notify clients in accordance with the Agreed Service Levels of any development that might have a material impact on our ability to provide the Services.</p> <p>We will not provide separate notices where we have already reported or otherwise communicated a failure to meet the Agreed Service Levels or to perform the Services in accordance with the Agreement.</p>
(c)	Business Continuity and Security	Clause 14	<p>We have included the following commitments in clause 14 of the Addendum, which closely reflect the requirement under Article 30(3)(c):</p> <ul style="list-style-type: none"> a commitment to implement, maintain and test appropriate business continuity plans at regular intervals. (Note that details of the BCP plans we have in place are set out in our Operational Resilience Compliance Statement); and a commitment to maintain ICT security measures, tools and policies that provide an appropriate level of security for the provision of Services. (Again, the Operational Resilience Compliance Statement describes what measures we have in place in line in this regard). <p>For more information on our approach to BCP, please see clause 3.1 of our general terms and here: https://policies.fundapps.co/fundapps-policy-portal/-LrODnq5HI65-TLW7fbC/fundapps-policies/business-continuity</p>
(d)	Threat-Led Penetration Testing	Clause 15	<p>We conduct our own annual pen tests which is outlined in our IS policies we contractually agree to abide by. See: https://policies.fundapps.co/fundapps-policy-portal/-LrODnq5HI65-TLW7fbC/fundapps-policies/infosec/vulnerability-management#vulnerability-detection</p> <p>We nevertheless agree to participate and fully cooperate in required TLPT conducted by financial entities where our services have been determined to support a critical or important function of a financial entity. TLPT can be disruptive and given that it impacts live production environments, a TLPT exercise implemented by a financial entity could impact other FundApps clients and also our subcontractors. We therefore require no less than 90 days' notice of a required TLPT exercise, a written agreement with the financial entity or an external tester, effective risk management controls in respect of the TLPT and compliance with FundApps policies and procedures for the TLPT, among other things.</p>

DORA Reference	Subject Matter	Addendum Ref.	Compliance Approach
(e)	Audit and Inspections	Clause 17	<p>FundApps grants the right to access, inspect and audit FundApps' performance of the Service and FundApps' compliance with the Agreement.</p> <p>FundApps does however require 30 days prior written notice, except in an emergency or crisis situation or at the requirement of a regulator.</p> <p>FundApps also requires some basic protection around any exercise of an audit rights, including that the client ensure that no third party appointed to conduct an audit is a competitor, to verify that the third party and its personnel exercising an audit have the necessary skills, knowledge and experience, and that a confidentiality agreement is entered into with FundApps.</p> <p>We also expect audit rights to be exercised in risk-based and proportional manner, taking into account the legal requirements, the context and the nature of the service provided.</p> <p>We do expect clients to first consider if other documentation, such as FundApps internal audit reports, third-party certifications and other information provides the required level of assurance before any client exercises an audit right. Alternative assurance levels will have to be agreed if an audit rights will affect the rights of another client of FundApps, including in respect of FundApps confidentiality obligations owed to others.</p> <p>FundApps expects reimbursement of fees and costs reasonably incurred in connection with the exercise of an audit right.</p> <p>See also our comments alongside the Article 28(6) requirements.</p>
(f)	Exit	Clause 18	<p>As contemplated under Article 30(3)(f)(i), we have provided for an ability for you to require that the Services continue for a transitional period of up to 3 months following the effective date of termination or expiry of the Agreement, subject to you continuing to pay in full for those Services.</p> <p>In addition, during the transitional period, if request by you we may agree to provide additional support and assistance to support an efficient and orderly transition of the Services to you or a replacement supplier. Any such support and assistance (including the applicable fees) will be agreed between us in a separate Order Form or similar document.</p> <p>You will separately need to put in place measures in the background to ensure that, for example, you can quickly engage a replacement supplier in the event that this Agreement is terminated / expires.</p> <p>We also provide Client Data on request in a readable format and in accordance with the terms of the Agreement.</p> <p>See also our comments alongside the Article 28(8) requirements.</p>