Pensions Dashboards Programme

Connection process and guidance

July 2022

pensionsdashboardsprogramme.org.uk

Money & Pensions Service

Contents

1. Background

Under the current legislative proposals put forward for occupational pension providers by the Department for Work and Pensions (DWP) and for providers of personal/stakeholder pension providers by the Financial Conduct Authority (FCA), UK pension providers (we use this as an umbrella term to cover both preceding categories).

Similarly, the legislation will require pensions dashboards services to connect to MaPS' ecosystem. Thereby, they will join the pensions dashboards ecosystem. For pension providers, this means they will be able to receive data from dashboards users for the purpose of searching and matching against users' pensions and allow their users to request and view their pensions information via a pensions dashboard service.

Qualifying pensions dashboard services (QPDS) are regulated by the FCA and connected to our ecosystem. This means they will be able to offer a pensions dashboard service and enable their customers to find their pensions using the central digital architecture to link up to the pension providers where users' pensions are located. As the FCA regulates the conduct of firms carrying out an activity, the FCA's Handbook rules will apply to QPDS firms and can impose standards on those firms (aligned to FCA's statutory objectives) when carrying out the qualifying pensions dashboard service. The FCA will consult on its proposed Handbook rules in due course.

MaPS is responsible for building and maintaining the central digital architecture that will make dashboards possible, connecting millions of users to their information from thousands of pensions providers, via multiple pensions dashboards. For more information about the pensions dashboards ecosystem and its components, see pensionsdashboardsprogramme.org.uk/ecosystem/.

To comply with the new obligations set out in the legislation, QPDS and pension providers must cooperate with the Money and Pensions Service (MaPS) to assist with the exercise of its functions in relation to pensions dashboards services, register with MaPS, and connect to MaPS (the digital architecture established by MaPS which makes dashboards possible). The Pensions Dashboards Programme (PDP) is an executive function of MaPS and is responsible for delivering these functions on MaPS' behalf.

The legislation also imposes several other duties on pension providers to receive requests from users to find their pensions, undertake matching to find any pensions the user has with them, to register found pensions for that user, and to then return information about these pensions to the user via their dashboard. Pension providers will not be able to comply with these other duties unless they have first complied with the duty to connect.

2. About this guidance

Status

This document sets out what connecting to the ecosystem will involve and explains what QPDS and pension providers should expect when connecting and the steps they will need to take. It also provides guidance on the likely duration of each step.

The draft legislation requires trustees/managers/authorised persons to have regard to this when they connect their pension provider to the pensions dashboards ecosystem. This means that while not strictly mandatory (as are standards), it carries legal evidential weight and authority, and failure to have regard for the guidance can be used as evidence of a breach of legal duties and may be used in regulatory action by the Pensions Regulator (TPR) or FCA. In effect, this means that pension providers must either follow this guidance or have good reason for departing from it and be able to demonstrate that they have achieved the same result via their alternative path. The proposed legislation also requires pension providers to keep a record of how they have carried out the steps set out in this guidance, or of alternative steps they have taken to achieve the same results, for at least six years from the end of the pension provider year to which they relate.

Audiences

This document is intended for:

- pension providers – ie trustees/managers of occupational pension providers and authorised persons responsible for providers of personal/stakeholder pension providers
- any third-party organisations pension providers may use to connect on their behalf
- QPDS

We expect that much of the implementation of the standards will be undertaken by such third parties (such as administrators or software providers) on behalf of multiple clients. In practice, therefore, the primary audience for implementing the processes and guidance set out here may be those third parties. However, the legislation requires the pension providers to have regard to this guidance, and they are therefore ultimately accountable, even if they delegate the implementation to a contracted third party.

3. Connection options and indicative timings: guidance for pension providers

The legislation will require pension providers to connect but does not prescribe the way to do this. There are two options: connecting direct or connecting via a third party.

Connect directly, building your own digital interface to the ecosystem

Establishing a new direct connection to the ecosystem is a significant undertaking and we recommend any organisations considering this option register their interest early with PDP to ensure a full understanding of the activities and requirement involved. Please get in touch infopdp@maps.org.uk.

If you are connecting directly via a new interface to the ecosystem, you will need to follow our procedures and processes set out in section 4 below for setting up a new endpoint (ie a new technical connection to the ecosystem) in their entirety. We estimate the time required to register and test an endpoint and successfully complete service acceptance prior to transition to the live environment to be 60-90 working days. This may differ depending on factors including the availability and experience of your key resources and your other competing organisational priorities.

For these reasons **if you intend to connect directly by setting up a new live endpoint, we recommend that you look to commence this process 6-9 months prior to** your staging deadline and ensure early engagement with PDP so that we can schedule a test window to complete the required activities.

You should also be aware that you may need to undertake some additional work to map or extract your underlying data to your endpoint. This can be done in tandem with the testing of your endpoint, but we recommend you assess and build in sufficient time to allow for this step, in addition to the steps to set up your endpoint, well in advance of your staging date.

Connect via a third-party organisation's interface to the ecosystem

We expect most pension providers to connect via a third-party data provider.[1] This could be an interface provided by an integrated service provider (ISP) which enables multiple pension providers to connect through a single (or set of) API connection(s), or an interface built by your existing third-party administrator or pension software provider.

In this case, you will not have to follow all the steps set out in section 4, as your third-party provider will have already completed the prescribed procedures and processes for onboarding to the test environment, completed testing, and established a live connection to the ecosystem. Your connection journey via a third party will therefore be much simpler and you will just need to register your connection to the existing endpoint provided by this third party.

You should allow up to 30 working days to complete registration and connection via an already-connected third party. (Note that for all but the first cohort of pension providers to be connected, this means you should come to PDP to begin your connection **before your pension provider's connection window opens**.) In practice, if all data are correct on the registration form and PDP are able to service the requested connection date, and we do not have capacity bottlenecks (due to others requesting to connect at the same time), it will be considerably less than this, and we expect the process of registering as a pension provider on the ecosystem connecting via a third party to take no more than a week.

You should also be aware that you will potentially need to undertake some additional work with your chosen third-party provider to map or extract your data to their endpoint. You should ensure that you work with your chosen provider to assess and build in sufficient time to allow for this step as part of your planning.

Requesting a date within your connection window

Whichever connection option you take, the legislation will require you to connect by a staging deadline, with pre-connection steps undertaken within a 'connection window'. For the first cohort of pension providers to connect, the connection window opens five months prior to the staging deadline. Thereafter, the staging deadline for occupational pension schemes is the date specified in the draft

[1] We use the broader term 'data provider' (rather than 'pension provider', which we use specifically for occupational pension schemes or personal pension providers) to refer to the organisations that provide the data to dashboards: this includes pension providers, third-party administrators and ISPs. Thus, all data providers connect pension providers, whereas pension providers may *not* be data providers themselves, but may use the services of a third-party data provider to connect them.

legislation (Schedule 2) being the latest date by which they must be connected to MaPS and the connection window is one month leading up to and including the staging deadline. You will need to take account of the steps we set out below and the indicative timings above to ensure you connect within your allotted connection window.

MaPS has responsibility for managing the connection of pension providers into the ecosystem, and you will need to cooperate with us so we can connect you within your window (or earlier, should you wish to apply to connect early – for which see our early connection guidance). This means that we may not necessarily be able to grant you your preferred connection date within the 'connection window' if multiple pension providers request the same date. You will need to apply for a connection date within your window, and we will do what we can to accommodate requests for specific dates but must manage these requests according to the demand and our capacity to service the requests and therefore cannot promise to grant first preferences.

4. Process for connecting directly

This section applies to:

- data providers:
    - pension providers connecting directly
    - third-party organisations connecting on behalf of pension providers
- QPDS

The connection journey for connection of a new endpoint (ie a new technical connection to the ecosystem, whether that is an endpoint for a single pension provider, or an endpoint for a third-party interface through which multiple pension providers will then connect, or a new dashboard), involves the following steps:

1. registering your organisation as a data provider/QPDS
2. onboarding to the test environment and compliance testing
3. service acceptance – including external pen testing
4. requesting a go-live date and transition to live

Registering your organisation as a data provider/QPDS

You will need to initiate your onboarding process using a publicly available registration link. You will need to have identified five main staff roles required to complete onboarding:

Role	Description	Key activities
primary business contact	the main representative of the organisation and the first contact to be registered, responsible for initiating the onboarding process on behalf of the organisation	• registering the organisation and managing pension providers • adding, deactivating and reactivating users

primary technical contact	the first point of contact for all technical issues including requesting and deploying certificates and resolving API endpoints being down	• request and deploy certificates
test manager	the representative responsible for managing conformance and compliance testing and providing approvals for the addition of pension providers to endpoints	• perform testing • review and upload test reports and documents
security lead	the main security representative of the organisation, responsible for attending the PDP Security Working Group to present IT health check test results	• get updates from testing from organisation • attend MaPS' Security Working Group
service management team	the team which will be engaged in managing service acceptance and the transition into live	• help clear service acceptance • cleardown of logs

Creating primary business contact account

This is necessary to gain access to the portal to begin the path to connection. Your primary business contact will need to access the publicly available PDP signup page and submit the following personal and organisational details to request an account:

Details	Data items
personal details	• first name • last name • mobile phone number • organisation email • employee number
company details	• registered company name • registered company number • building and street • town or city • postcode • organisational landline telephone number
ICO data protection registration details	• data protection public register number • building and street • town or city • postcode
details of pension provider that you will be acting for in connecting to the ecosystem *(does not apply to QPDS)*	• regulating body • PSR number for TPR-regulated pension providers/ firm registration number for FCA-regulated providers • registration code

PDP will then validate the new user's credentials and approve the request. Following approval of the new account, PDP will provide your primary business contact with a one-time security code, which they will use to set up an account with PDP's platform. They will create a permanent password for this user account.

Register your organisation and endpoint(s)

Your primary business contact can then initiate a request to register your organisation, including endpoint(s) to be used for connection, on the PDP test platform. They will complete the registration form. This includes providing organisational details (eg registered company name, provider type), endpoint information (URLs for test endpoints and live endpoints).

You will also have to sign to confirm acknowledgement of, and your adherence to, the code of connection (the security, service, and operational standards with which the legislation requires you to comply). Your primary business contact will then request an update to the governance register to acknowledge your endpoint.

Data providers will also need to provide information relating to the pension provider on whose behalf they are connecting, including the PSR number or FCA number, staging deadline, holder name (that is, the permanent identifier which is used to represent the URL of the view endpoint from which pension information is served to dashboards), along with the regulator-issued registration code for a UK pension provider on whose behalf they are connecting to the ecosystem. We will then check the registration code against the code we are given by the regulator and if they match, we will confirm registration and approve your progression to testing.

Similarly, QPDS will need to provide their FCA firm reference number and a registration code, which assures PDP they are authorised to provide a pensions dashboard service.

Creating service manager, test manager and additional user accounts

Once your primary business contact has set up an account and registered your organisation as a data provider/QPDS, they may request additional user accounts (you will need the five roles mentioned above in 4.1). To create additional accounts, your primary business contact must request their creation, using their own account. They will need to provide the users' personal and organisational details (as above) and role(s) for the requested additional users. PDP will then validate the new users' credentials and approve the request(s). Following approval of the new account(s), your primary business contact will then be provided with a one-time security code for each new user, which they will need to communicate to the new users, who in turn will use this to set up their own accounts with PDP's platform, via a link sent directly to the new users' provided email address. They will create a permanent password for this user account.

Testing

Once registered as a data provider/QPDS provider, you may request the cryptographic package (ie the materials for testing) for the test environment and commence testing. You may initially carry out conformance testing, which is internal 'sandbox' testing performed by you to check your compliance with the API standards in a PDP test bed. You will then need to go through compliance testing. This is formal testing, required and witnessed by PDP, to prove compliance with the API standards. You will

need to provide a test plan and test scripts for review by the PDP test manager. (The PDP test manager will provide test scripts which you are recommended to use. If you opt to use your own scripts, you will need to be able to demonstrate how your alternative scripts achieve the equivalent outcome.) Your test manager will then use these scripts to carry out compliance testing. Your test manager will also need to attend daily test calls run by the PDP test manager for the duration of your compliance testing, and you will need to provide a written report to the PDP test manager to exit compliance testing.

You will be required to submit evidence from audit logs and test results to PDP to prove your compliance with the API standards to be granted permission to proceed to service acceptance.

Service acceptance

Having completed compliance testing, you will then need to go through formal service acceptance, the first step of which is to demonstrate you meet the cyber security requirements for your connection to the dashboard ecosystem through our service acceptance process.

As required by our security standards, you will need to undergo a penetration test (also called an IT health check) to assess your interfaces' security. This is a simulated cyber-attack or 'ethical hacking', carried out by an independent third-party expert in cyber security, designed to check the interface to identify and address any exploitable security vulnerabilities. Our security standards require you to use a provider accredited by the Council for Registered Ethical Security Testers (CREST) to undertake this test and prescribe the minimum scope for this test.

Your security lead will need to compile the evidence of your IT health check testing by a CREST-accredited provider, submit this to the PDP Security Working Group, and attend the Working Group to present the evidence for review. Our security standards require that your IT health check test does not flag any medium- or high-risk vulnerabilities: the test report will need to demonstrate only low-risk vulnerabilities identified (if any) in order to meet the required standard. (You will also be expected to have a plan to address any low-risk vulnerabilities, and these should be resolved by the next [annual] IT health check, as per the security standards.) If any medium- or high-risk vulnerabilities are identified that have not been addressed, you will not be permitted to pass service acceptance, and will need to address the issues, undergo a further test, and return to the Security Working Group with a clean report showing no medium- or high-risk vulnerabilities.

Once you have presented your IT health check evidence demonstrating compliance with the standard required, you will be approved by the Security Working Group chair to proceed to the final stage of service acceptance. Your service manager will complete a service acceptance pack and submit to the PDP IT service manager.

Your service manager will then update and finalise a change request. Once approved, your primary business contact will be able to register a request for the cryptographic package containing the necessary certificates and keys for the live environment.

Transition to live

You are now connected and part of the ecosystem, operating in the live environment. For pension providers/QPDS, this means you will now be receiving find requests and expected to undertake

matching against all requests received. For QPDS, this means you will now be able to offer your pensions dashboards service to users, provided all you have obtained FCA authorisation.

For the first two weeks of operating in the live environment, you can expect enhanced support from PDP to monitor your endpoint stability. This includes use of live monitoring tools by PDP to ensure that your endpoints are up and running and performing to service levels.

5. Process for connecting via a third party

This section applies to:

- *pension providers connecting via a third party*

Once an endpoint has been successfully set up and transitioned into the live environment, following the connection process set out above in (4), pension providers can register and connect via this connection.

The draft legislation requires pension providers to register with MaPS. This is important because we have a responsibility to ensure that only legitimate parties (ie regulated pension providers or third parties implementing their duties on their behalf) can access the dashboards ecosystem, and the governance register works to gate-keep the ecosystem. The governance register ensures that all the entities within the ecosystem are registered and monitored to ensure they operate correctly and securely, and it allows access to be revoked if any party is found to be operating incorrectly.

If you are connecting to MaPS and the ecosystem via a third-party organisation that already has a connected interface to the ecosystem (following the process above in section 4), the whole process is much simpler.

You will need to ask your contracted third party's primary business contact to initiate your addition to their existing endpoint. (Thus, all pension provider registrations are initiated by a data provider's primary business contact.) Your third-party provider's primary business contact will complete a registration form and request an update to the governance register to associate your pension provider with the live endpoint. You will need to provide your PSR number/FCA number and regulator-issued registration code(s) to your third-party provider to be included in the registration form. This is essential to assure us that we are only connecting legitimate pension providers.

Your third party's primary business contact will submit the registration form and request the update to the governance register. We will then check your registration code against the code we are given by the regulator for your pension provider. We will also check your staging deadline (if you are seeking to connect outside of your connection window, you will need to have regard to our guidance on early connection).

You will need to satisfy yourselves that the third party has gone through the necessary service acceptance processes and has met the required security standards on your behalf but will not need to go through these processes yourselves. Your third party will need to do the following on your behalf:

1. provide the pension provider information required to register
2. confirm the third-party provider's IT health check test still holds (the primary business contact will need to upload an assurance letter to confirm that the IT health check on the interface is still valid)
3. submit an operational change request via the PDP platform to associate the pension provider with the endpoint

We will then process this change request and (provided the necessary information is all present and correct), provide your third party's primary business contact with a scheduled transition date and notification of the update to the governance register. You will now be associated in the governance register with the third-party data provider you are connecting via and will be connected to the ecosystem.