Australian Government
Australian Taxation Office

DSP De-Whitelisting Process

Digital Partnership Office

Contents

VERSION CONTROL

Version	Release date	Author	Description of changes
1.0	20/12/2019	Digital Partnership Office	
1.1	01/04/2020	Digital Partnership Office	Minor update to content and process flow diagram, specifically contacting DSP clients.

Introduction

All SBR-certified software products must be whitelisted to utilise ATO production services.

Whitelisting enables the ATO to manage the use of our services, which may include de-whitelisting where required. De-whitelisting is the process of suspending or removing access to the ATO production or test environments.

De-whitelisting may occur where a Digital service provider (DSP) is not compliant with our requirements or where a cyber incident presents a risk to our digital wholesale channel, ATO reputation or taxpayers.

The ATO will always endeavour to work through identified issues with DSPs. However, a failure to respond and adequately address issues will result in de-whitelisting. The SBR Conditions of Use enables the ATO to lawfully suspend or terminate any software product, report or information from access to SBR services.

The purpose of this document is to provide clarification on the situations and process of de-whitelisting. It considers the triggers, response and factors for re-whitelisting.

De-whitelisting triggers

De-whitelisting can be initiated for several different reasons. The type of de-whitelisting that occurs is dependent upon the unique circumstances of each case.

The triggers for de-whitelisting include:

1. **ATO initiated immediate de-whitelisting** will occur where the data held by a DSP or their systems have been compromised, resulting in the loss of either of the following:
    - Confidentiality of tax and super data
    - Integrity or availability of ATO digital wholesale channels

2. **ATO initiated delayed de-whitelisting** will occur where immediate de-whitelisting is not required. As part of this process the ATO will:
    - Provide written and verbal notification to the DSP of the issue(s) and actions required
    - issue the DSP with an initial warning of the intent to de-whitelist, including the proposed date for de-whitelisting
    - notify the DSPs clients of the intent to de-whitelist
    - issue a final notice to the DSP that includes a scheduled date for de-whitelisting actions to occur. Usually DSPs are provided seven (7) to fourteen (14) days for action to take place, however this will depend on the volume of transactions made by the DSP's clients
    - issue a notification to inform the DSP that de-whitelisting has occurred

In addition to the above ATO initiated reasons, a DSP may also request de-whitelisting of their product(s) should it be required.

3. **DSP initiated de-whitelisting** can be either immediate or delayed/scheduled at the request of the DSP. DSPs can request de-whitelisting of their product(s) by:
    - Contacting their DPO Account manager directly
    - Logging a request via Online Services for DSPs
    - Emailing DPO@ato.gov.au

Security incidents

Digital service providers are required to report all cyber security incidents to the ATO. Where security incidents arise, the ATO may de-whitelist a DSP product or access to a single service (API).

The ATO's reputation as a secure data custodian is integral to ensuring taxpayer's confidence and the use of digital platforms and technologies continue to be a secure and contemporary experience.

There are several ways a security incident may be identified. These include but are not limited to:

- ATO Cyber Security monitoring
- direct notification from impacted DSPs
- direct notification from impacted taxpayers, employers or super funds
- direct notification from impacted tax or BAS agents.

The severity of security incidents is also a factor for consideration, this includes:

1. **A major security incident** is an event where a DSP's system or data security have been compromised, resulting in loss of confidentiality of tax and superannuation related data or loss of integrity or availability of ATO digital wholesale channels. This includes issues within a DSPs product that cause disruptions to ATO wholesale services

    This will result in immediate de-whitelisting.

2. **A moderate security incident** is an event where a DSPs system may have been compromised, however the tax or superannuation related data either remains secure or very limited exposure.

    This may result in delayed/scheduled de-whitelisting.

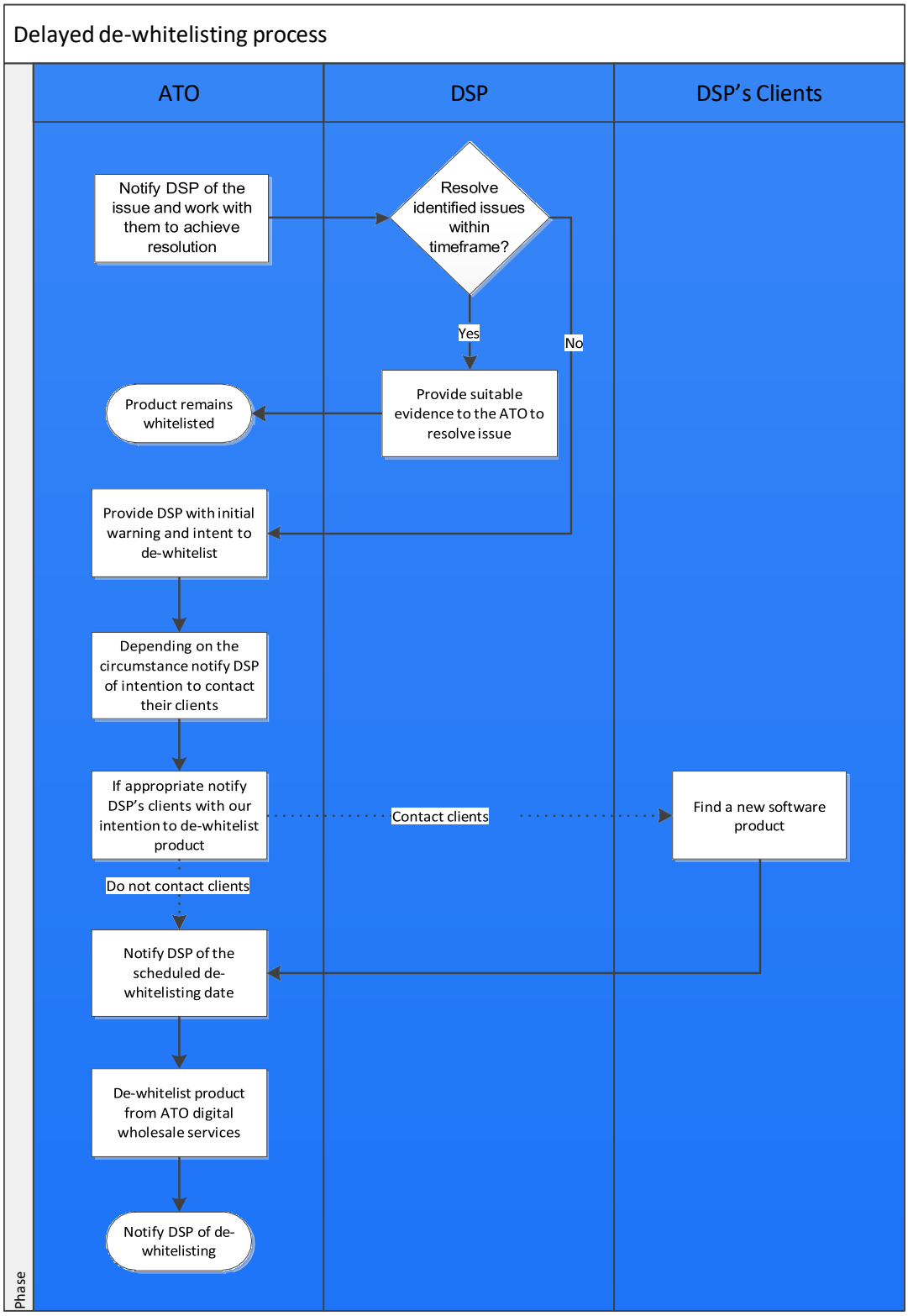
De-whitelisting circumstances

Circumstances where a DSP may be de-whitelisted includes but is not limited to:

Event	Immediate de-whitelisting	Delayed de-whitelisting
Major security incident	Yes	N/A
Moderate security incident	Potential	Potential
Non-compliance with mandatory obligations. This may include: • DSP Operational Framework • Product Verification Testing • Data quality • Service specific terms and conditions (eg SuperTICK, SuperMatch and MAAS)	No	Yes
Breach of fair use of ATO systems	Potential	Potential

Process of delayed de-whitelisting

The following process outlines a general approach; however, each de-whitelisting will be dependent on the specific circumstances.



Notification of de-whitelisting

The notification of de-whitelisting provides a DSP with:

- Details non-compliance and/or security incident
- The issues that need to be addressed and timeframes for the DSP to provide the ATO with suitable evidence
- Date when the ATO will inform a DSP's clients of the de-whitelisting (if applicable)
- Scheduled de-whitelisting date
- Confirmation of processed de-whitelisting.

Re-whitelisting - considerations

Following de-whitelisting, if all appropriate actions are taken by the DSP to rectify the issues, re-whitelisting may be considered. For a DSP to be re-whitelisted the following must occur:

- The DSP must provide the DPO written assurance and appropriate evidence that they have rectified the issue which was the cause of their de-whitelisting
- The assurance and evidence will be assessed by the ATO and a decision will be made to accept/refuse the re-whitelisting request
- Where applicable, the DSP must complete the latest Security Questionnaire to make sure that they have the right security posture. This includes compliance with any outstanding requirements under the DSP Operational Framework
- Where required, the DSP may need to perform Production Verification Testing (PVT) of their product to ensure correct execution of their code. In some cases, an abbreviated PVT process can take place, however this will be determined on a case by case basis