Code 15 Guidance note - Due diligence, risk assessment and control (DDRAC) Standard

The DDRAC Standard acknowledges the importance of effective DDRAC processes which are central to good business practice as it enables all parties in the value chain to operate with confidence and assurance that the practices of those they contract with in the delivery of phone-paid services are compliant and effective.

This guidance note sets out the PSA's expectations and provides more detail on how phone-paid service providers (network operators, intermediary providers and merchant providers) can comply with the Due Diligence, Risk Assessment and Control (DDRAC) Standard and Requirements. It provides more detail on:

- what to include in effective due diligence policy and procedures
- undertaking initial risk assessments
- what ongoing risk assessment and control processes need to be in place for the lifetime of any particular service/contractual arrangement
- storage of information
- responding to incidents, including terminating contracts.

If you have any queries about the guidance set out in this note or want to discuss your approach to compliance with the DDRAC Standard, please email us at compliance@psauthority.org.uk.

In summary, the responsibilities of the different parts of the value chain are as follows:

Network operators are required to perform DDRAC on any intermediary, merchant, third-party verification platform, or affiliate advertiser with whom they are directly contracted.

Intermediary providers are required to perform DDRAC in respect of any contracted downstream party involved in the provision of a particular service. This includes any other intermediary provider, third-party verification platform, affiliate advertisers or merchant provider with whom they are directly contracted.

Merchant providers may be required to perform risk assessment and control on clients with whom they are directly contracted to facilitate the provision of a service, this includes affiliate advertisers and any outsourced customer care facilities. Merchant providers should note that while they are not directly required to do so by the Code, they may, through any contractual arrangements with network operators or intermediaries, be obliged to perform DDRAC on any third-party they contract with who is involved in the provision of a service, as per Code Requirement 3.9.12).

All information gathered in respect of due diligence, and/or risk assessment and control must be made available to the upstream value chain and the PSA on request.

DDRAC policies and procedures

Network operators and intermediary providers must have clear and effective DDRAC policies and processes in place. While merchant providers are not required by the Code to have due diligence policies and processes in place, they may be contractually required through the value chain to put them in place in addition to the risk assessment and control policies and processes they should have in order to meet their obligations under Code Requirement 3.9.2.

We recommend that DDRAC policies and procedures set out:

- the information that the network operator or intermediary provider will collect as part of due diligence, prior to a commercial relationship commencing. This should include the information listed at Code Annex 2.3.
- how such information will be verified and retained
- how information will be used to undertake the initial risk assessment
- the circumstances in which a provider may make additional enquiries of parties that they contract with, e.g. where the information provided as part of due diligence processes flags risks or issues that require further investigation
- the checks and verification measures that must take place prior to making a migrated service available to consumers
- the processes and timeframes for when and how a provider will review the information it holds to ensure it is up to date
- how risks will be recorded – in the case of an issue, the explanation should set out exactly when and how it was discovered, and by whom
- how identified risks will be responded to, and the steps that should be taken to prevent potential consumer or regulatory harm – this should include a timestamped record of who has signed them off as being completed and when
- how incidents will be recorded
- a procedure or action plan which sets out how the provider will respond to issues of suspected or evidenced consumer harm and/or non-compliance. This includes ensuring that any contractual requirements are being complied with, and that information is shared between the parties in a timely manner.
- the circumstances in which contracts may be terminated, and the process surrounding notification of such termination. This should include clear, documented consideration of whether intermediary or merchant providers should be suspended or have their contracts terminated in relation to more services incidents and clearly documented

consideration of whether a sequence of incidents warrants suspension or contract termination.

- who in the organisation has the overall responsibility and oversight for reviewing DDRAC information, including the authority to take decisions including sign-off – a director or the equivalent person with responsibility for DDRAC within the organisation
- who in the organisation is responsible for reviewing DDRAC processes on an ongoing basis to ensure they remain fit for purpose and are operating effectively – a director, or the equivalent person with responsibility within the organisation.

DDRAC policies and procedures should be version controlled (where updated over time) and provided to the PSA on request.

Due diligence – pre-contractual enquiries

The PSA expects parties in a value chain to carry out effective due diligence before contracting with another party to provide a phone-paid service, and to use this information to undertake a risk assessment on each of their clients and services. The purpose of undertaking due diligence before a commercial agreement commences, or a service is accessible to consumers, is to ensure that providers fully understand the organisations they contract with in the delivery of a phone-paid service.

A non-exhaustive list of the types of information to be collected as part of due diligence checks can be found at Annex 2 of the Code. The requirements at Annex 2 represent the minimum level of information to be collected where such information exists and is obtainable. Should a network operator or intermediary provider deem additional information is appropriate in certain circumstances to satisfy its own due diligence requirements, Annex 2 does not preclude or otherwise limit the scope of information that can be collected.

This information should be retained as set out in our data retention notice and remain available to the network operator or intermediary provider as relevant, to enable their own assessment of the due diligence performed by their contracted parties on other participants involved in the provision of each service.

As required by Code paragraph 3.9.6, network operators and intermediary providers are only required to undertake DDRAC on those parties with whom they have a direct contractual relationship. We do not expect network operators and intermediaries to have any downstream responsibilities for third parties with whom they do not have any direct contractual relationship. But what we do expect network operators and intermediary providers to do is include in their contracts (Code paragraph 3.9.12) a requirement that the parties they contract with include DDRAC obligations in their own contracts with others involved in the provision of the services. It is in this way that DDRAC flows from network operator to intermediary and on to other parties in the value chain which could include other intermediaries, merchants or third parties.

Where a network operator or an intermediary provider does not have a direct contractual relationship with a party not directly within value chain (for example, a third-party verification

platform or an affiliate marketer), we expect the party who contracts with the third party to include due diligence requirements in their contract. There should also be arrangements that enable sharing of due diligence information across the value chain to assist all parties in the value chain to be able to assess any potential risks effectively.

Where a network operator or intermediary provider contracts with an app store, we do expect that the network operator or intermediary provider has a good understanding of what checks, systems and processes contracted parties have in place to ensure that third-party app store services are unlikely to cause potential harm. But this does not mean that network operators or intermediary providers are responsible for conducting DDRAC in respect of all the apps/games which are available through that app store.

The use of third-party compliance or auditing houses does not absolve providers of their DDRAC responsibilities. The use of such companies may assist with the ongoing risk assessment that networks and providers are expected to undertake, for example by providing monitoring of services, but on its own is unlikely to be considered sufficient.

Providers using third parties to undertake monitoring should ensure they undertake due diligence on such companies aligned with the expectations as set out in Code Annex 2 and supported by this guidance.

We recommend that network operators and intermediary providers take steps to understand the particulars of the services being operated on an ongoing basis. This should include network operators and intermediary providers collecting, and keeping up-to-date, information on the service types being offered by providers and whether any of those services fall into categories of service subject to service-specific Requirements. Network operators and intermediary providers should ensure that they are fully aware of the services being provided, inclusive of any specific requirements which may be applicable to that service type or payment mechanism. For example, where number ranges are allocated by a network to an intermediary for voice services, the network in question should ensure they are fully aware, through the intermediary provider, of the types of services their merchants are using the numbers for, as well as any specific requirements which may be applicable to those service types, for example, the recording of live entertainment services or any applicable call length or spend limits.

Using due diligence information to undertake an initial risk assessment

The information collected as part of due diligence enquiries prior to a contract commencing or prior to a service going live should be used by the relevant party to develop an initial assessment and/or risk score in relation to that party, the value chain overall and the relevant services. This will enable them to put in place appropriate risk controls to ensure the compliant delivery of phone-paid services to consumers.

Generally, we consider that all new clients and/or services would be likely to need a greater level of risk control than established services. This is on the basis that there is often limited information on which to base the initial risk assessment. The risk score or rating should also consider:

- the service type being delivered

- the length of time a provider has been active in the phone-paid services market – both in the UK and in other markets
- the compliance history of the party or any breach history relating to the service if they have been active in the UK market before
- the processes in place for addressing any issues and sharing information across the value chain to ensure any issues are dealt with promptly and effectively.

As the relationship and experience with the client develops, the assessment of the level of risk that the client and/or service(s) pose can be adjusted. We recommend that network operators, intermediaries and merchant providers review risk assessment and control processes periodically to ensure that they remain effective. The review period will depend on each client; the confidence established through ongoing relationship, the complexity of the role within the value chain and any risks associated with the service offered. Where longer intervals between periodic reviews on a particular client are established, this should be on the basis that an extended period between reviews can be fully justified and evidenced should issues come to light.

Risk assessment and control

The PSA recommend that any party undertaking DDRAC should have a process for risk assessment in place for each of their clients and each service that the client is operating. Ongoing risk assessments are dynamic and need to be responsive to the information that is shared across the value chain. For example, a merchant provider may be considered to have a low risk profile if they have operated services with limited issues over a long period. But if that merchant provider wants to operate a new service type where the level of risk is yet to be established, we recommend that this be taken into account and monitored closely until there is sufficient data available to evidence that the service is operating effectively.

Agreements should be in place between parties in the value chain to enable information to be shared as per Code Requirement 3.9.10, so that risks can be identified and steps taken to mitigate them.

We recommend this includes information about both the services being operated and the organisation operating them. For example:

- information about changes to the method of promotion or sign-up
- numbers of consumers using a service
- complaints data
- refunds processes and procedures, and data on refunds issued (including any goodwill payments made)
- information about any breaches being investigated by the PSA
- alterations to the company structure or appointments of new staff in key positions

- alterations made to the service and/or promotional methods.

Network operators, intermediary providers and merchant providers should be able to demonstrate that this information has not been tampered with in any way and has been securely stored since the records were created. Network operators, intermediary providers and merchant providers within the value chain should undertake their own checks and monitoring or have access to information as needed to satisfy themselves that the service is operating effectively. Internal checks should be undertaken when there are unusual patterns of activity which may indicate consumer harm (e.g. spikes in traffic and/or consumer complaints made directly to the provider of the service).

Network operators, intermediary providers and merchant providers should periodically test and/or monitor risks, as appropriate to a particular provider or third party or service category (e.g. for a subscription service, it may be prudent to test the clarity of promotions, and whether receipts have been sent). We recommend that risks be recorded and updated in a risk register or equivalent document.

The frequency of such testing should be based on the risk assessment. For example, it may be appropriate to monitor a client with no breach history, or where none of the directors are linked to other companies with breaches, or where the service type is considered lower risk, less frequently than where those factors exist. However, a dynamic assessment will need to be made, based on up-to-date information shared between the parties.

We recommend that network operators, intermediary providers and merchant providers have in place and periodically review:

- a procedure or action plan which sets out how the contracted party will respond to issues of suspected or evidenced consumer harm and/or non-compliance. This includes ensuring that any contractual requirements are being complied with, and that information is shared between the parties in a timely manner
- a plan for how the client's service or activity will be periodically monitored, based on the risk assessment, which includes:
    - monitoring to check that agreed promotional material and promotional methods being used match those seen by consumers
    - ensuring that complaint-handling processes are effective, timely and consistent.
- processes to ensure that the intermediary provider or merchant provider (as relevant) responds to any PSA request in a timely manner
- internal mechanisms to enable "whistleblowing" by staff, where appropriate.

This action plan/procedure should be reviewed from time to time and at least annually, to ensure it is operating effectively and enabling network operators, intermediary providers and merchant providers to assess and respond to risks as required.

Storage of information

All procedures for DDRAC should set out proper processes for collecting and storing the information gathered. All DDRAC evidence obtained should be:

- collated and retained in a dedicated and secure location
- backed-up to prevent data loss.

All relevant information in relation to a particular organisation/service should therefore be able to be accessible and provided in an appropriate format when requested by PSA.

Measures should be taken to ensure that evidence to support due diligence, risk assessment and control processes does not become inaccessible due to staff changes, human error, or technical failure.

Providers should ensure that they refer to and comply with the data retention notice issued by us which sets out the various categories of data that must be retained and the applicable retention periods.

Responding to incidents

We recommend that network operators, intermediary providers and merchant providers respond to incidents proactively and in line with their established procedures. We recommend that parties work closely with us in line with our supervision and engagement activities, and with other parties in the value chain to identify, mitigate and rectify any issues, including providing support to consumers.

Breaches should be identified and notified promptly to the PSA when they arise so they can be remedied, and services therefore delivered to a high standard to consumers.

To limit and address consumer harm, providers are encouraged to proactively alert us to any incidents regarding its own or third-party services. We will consider proactive cooperation when deciding about the most appropriate action to take (if any). Should enforcement action be deemed necessary, such cooperation will be considered as a mitigating factor.

Contracts

Network operators must have contracts in place which allow them to suspend or terminate their contractual relationship with intermediary providers in circumstances where non-compliant activity is discovered (Code Requirement 3.9.8). In addition, they should take effective action against intermediary providers whose platforms facilitate non-compliant activity, such as charging consumers without consent or where they reasonably suspect this to be the case.

This should include clear, documented consideration of whether intermediary providers should be suspended or have their contracts terminated in relation to more serious incidents and clearly documented consideration of whether a sequence of incidents warrants suspension or contract termination.

Intermediary providers should have contracts in place which allow them to suspend or terminate their contractual relationship with any merchant or third party consent verification platforms based on non-compliant activity, or where they reasonably suspect that such activity has or is occurring (Code Requirement 3.9.9).

This should include clear, documented consideration of whether merchant providers or third parties should be suspended or have their contracts terminated in relation to more serious incidents and clearly documented consideration of whether a sequence of incidents warrants suspension or contract termination.