Zellis Background Checking: Service Description Guide.

2024 edition

Contents

Document Control

Information	
Document Id	Background Checking SDG
Document Owner	Zellis UK Ltd
Issue in	November 2024
File Name	Zellis Background Checking Services Description – 1.2

1 Introduction

1.1 Scope

This document provides a detailed **Service Description Guide** "SDG" for the Zellis Background Checking Service. The **Customer Agreement** specifies which Services and options you have purchased.

1.2 Service rights

We grant to you, the Customer, for the Term, on and subject to the terms and conditions of this Agreement a non-exclusive, non-transferable right to access the Services, subject to the limits on Employees and Volumes set out in the Customer Agreement.

1.3 Updates to this Guide

We may amend or update this Service Description Guide from time to time including (without limitation) to reflect ongoing service enhancements. Changes will be made available to all Customers via the link in the Customer Agreement and notified to registered users through the Customer Help Centre. Each update will replace any previous versions. In the event of any conflict between this paragraph and the Terms and Conditions, this paragraph shall prevail to the extent of such conflict.

1.4 Service Descriptions

Each service is defined using the following standard format:

Ref: XXnn	Standard/Optional	Name
Our responsibility:		*Narrative describing Zellis' obligations*
Your responsibility:		*Narrative describing Customer's obligations*
Assumptions:		*Narrative describing applicable assumptions*
Exclusions:		*Narrative describing applicable exclusions*

Where:

- **Ref:XXnn** is the formal reference for the obligation comprising letters and numbers
- **Standard/Optional** defines whether a service is standard or may have been procured as an optional extra

2 Services

2.1 Background Checking

Background checking services can be procured on a stand-alone basis or as additional scope to augment Managed Payroll Services.

Ref: PC1	Standard	UK Standard Identity and Financial checks
Our responsibility:		Undertake UK standard identity and financial checks to be performed following the candidate submitting data onto the Background Checking platform, verifying all disclosed addresses by the candidate and any linked addresses or aliases for the last 6 years or more. The report will show any county court judgments, bankruptcies, insolvencies or voluntary arrangements within this period.
Your responsibility:		Request the UK Standard and Financial check when required against a role or candidate. Provide accurate contact information for the candidate.
Assumptions:		Candidate provides data in a timely and accurate manner.
Exclusions		Changes to candidate data, chasing of candidates to input information.

Ref: PC2	Standard	Employment checks
Our responsibility:		Verify all periods of employment during the agreed period. Verify contact information for previous employers and submit reference request typically covering name, employment status, period of employment, position on leaving and would they re- employ.
Your responsibility:		Request employment verification when required against a role or candidate. Provide clear detail of the period of time that requires verification. Provide accurate contact information for the candidate.
Assumptions:		Candidate provides data in a timely and accurate manner.
Exclusions		Changes to candidate data, chasing of candidates to input information.

Ref: PC3	Standard	Employment gap checks.
Our responsibility:		Identify and verify gaps in employment as agreed with Customer. Independently verify contact information for confirmation of activities and submit reference request or obtain supporting evidence.
Your responsibility:		Give clear instruction to Zellis Background Checking as to which period of time needs to be verified. If gaps are to be covered, stipulate for what length of time (e.g. 28 days; 3 months). Confirm to Zellis what methods are acceptable in absence of being able to verify a period of employment i.e. document collection. Provide accurate contact information for the candidate.
Assumptions:		Candidate provides data in a timely and accurate manner.
Exclusions		Changes to candidate data, chasing of candidates to input information.

Ref: PC4	Standard	Personal references
Our responsibility:		Obtain personal references against a candidate.
Your responsibility:		Request a personal reference when required against a role or candidate. Provide accurate contact information for the candidate. Qualify appropriateness of personal references offered.
Assumptions:		Candidate provides data in a timely and accurate manner.
Exclusions		Changes to candidate data, chasing of candidates to input information.

Ref: PC5	Standard	FCA full and frank reference.
Our responsibility:		Obtain a full and frank references for Financial Conduct Authority (FCA) registered roles. Independently verify contact information for previous employers responsibility to provide it.
Your responsibility:		Provide clear instruction as to when an FCA registered role is required for verification. Provide accurate contact information for the candidate.
Assumptions:		Candidate provides data in a timely and accurate manner.
Exclusions		Changes to candidate data, chasing of candidates to input information.

Ref: PC6	Standard	FCA services register check.
Our responsibility:		To check a candidate against the FCA services register database and report back on data found.
Your responsibility:		Provide clear instruction as to when a candidate requires checking against the FCA services register. Provide accurate contact information for the candidate.
Assumptions:		Candidate provides data in a timely and accurate manner.
Exclusions		Changes to candidate data, chasing of candidates to input information.

Ref: PC7	Standard	Basic criminal record check.
Our responsibility:		Carry out a basic criminal record check on the candidate via the Disclosure and Barring Service (DBS), or Disclosure Scotland (DS) if appropriate. Ensure all data is submitted to either the DBS or DS accurately and within the agreed time period.
Your responsibility:		Accurate data submission. Provide clear instruction as to when a basic criminal record check is required and supporting documentation if agreed. Provide accurate contact information for the candidate.
Assumptions:		A basic criminal record check. Details any convictions considered unspent under the Rehabilitation of Offenders Act 1974.
Exclusions		Changes to candidate data, chasing of candidates to input information.

Ref: PC8	Standard	Standard criminal record check.
Our responsibility:		To carry out a standard criminal record check on the candidate via the Disclosure and Barring Service (DBS), or Disclosure Scotland (DS) if appropriate. Ensure all data is submitted to either the DBS or DS accurately and within the agreed time period.
Your responsibility:		Accurate provision and upload of relevant documentation. Provide clear instruction as to when a basic criminal record check is required and supporting documentation. Confirm that the role that the candidate is applying for fits within the agreed criteria. Provide accurate contact information for the candidate.
Assumptions:		A standard criminal record check is used for those undertaking Controlled Function, SMCR Role, or other Specialist Requirements.
Exclusions		Changes to candidate data, chasing of candidates to input information.

Ref: PC9	Standard	Enhanced criminal record check.
Our responsibility:		Carry out an enhanced criminal record check on the candidate via the Disclosure and Barring Service (DBS), or Disclosure Scotland (DS) if appropriate. Ensure all data is submitted to either the DBS or Disclosure Scotland accurately and within the agreed time period.
Your responsibility:		Accurate provision and upload of relevant documentation. Provide clear instruction as to when an enhanced criminal record check is required and supporting documentation. Confirm this role fits within the agreed criteria. Provide accurate contact information for the candidate.
Assumptions:		This check is appropriate for those who may come into contact or work with those defined as vulnerable.
Exclusions		Changes to candidate data, chasing of candidates to input information.

Ref: PC11	Standard	Academic qualification check.
Our responsibility:		Verify a candidate's academic qualifications are within the criteria agreed with Customer. Independently establish contact information for the establishment and send request to the body that has authority to provide it within the establishment.
Your responsibility:		Provide clear instruction as to when an academic qualification check is required. Provide accurate contact information for the candidate.
Assumptions:		Typically confirms period of attendance, type qualification gained subjects and grades achieved.

Ref: PC12	Standard	Professional membership check.
Our responsibility:		Verify a candidate's current professional memberships. Independently establish contact information for the establishment and send request to the body that has authority to provide it within the establishment.
Your responsibility:		Accurate data submission. Provide clear instruction as to when a professional membership check is required. Provide accurate contact information for the candidate.

Ref: PC13	Standard	Sanctions check.
Our responsibility:		Put a candidate's identifying data through the database that screens for Sanctions and Politically Exposed Persons (PEPs) and report back on matches returned.
Your responsibility:		Provide clear instruction as to when a sanctions check is required. Provide accurate contact information for the candidate.
Assumptions:		Identifies sanctions, enforcements and warnings in the UK and worldwide.

Ref: PC14	Standard	UK directorships check
Our responsibility:		Put a candidate's identifying data through the database that illustrates any directorships held currently or historically and report back on data found.
Your responsibility:		Provide clear instruction as to when a check of UK directorships is required. Provide accurate contact information for the candidate.
Assumptions:		Provides company name, number and address for each directorship.

Ref: PC15	Standard	Adverse media search
Our responsibility:		Put a candidate's identifying data through the database that screens for any agreed areas of concern and report back on data found.
Your responsibility:		Provide clear instruction as to when a check of adverse media is required. Provide accurate contact information for the candidate.
Assumptions:		Reveals any negative information publicly recorded on the individual.

Ref: PC16	Standard	Proof of eligibility to work/passport.
Our responsibility:		Verify copies of good quality documentation images supporting the candidates Proof Of Right To Work in the UK. This includes processing via IDSP those documents that have an MRZ (Machine Readable Zone).
Your responsibility:		Provide clear instruction as to when proof of eligibility to work check is required. Candidate to provide copies of documentation and details
Assumptions:		A detailed inspection report is saved to the Background Checking platform should the Customer need to furnish the UK Borders Agency with this.

Ref: PC17	Standard	Digital Right to work identification and verification
Our responsibility:		Where the Service is provided by Zellis: provide digital right to work identification and verification checks. Where the Service is provided as a Partner Service: this service is provided by Trust ID and not part of the Zellis agreement.
Your responsibility:		Where the Service is provided by Zellis: Candidate to provide data and identify verification documentation to Zellis for screening. Customer to comply with the Digital Right to Work Terms set out in Annex A of this SDG. Where the Service is provided as a Partner Service: Candidate to provide data and identify verification documentation to Trust ID for screening

Ref: PC18	Standard	Driving licence check.
Our responsibility:		Run a check on a candidate's driving licence, highlighting any penalties, convictions of disqualifications and confirming its validity and report back on data found. Note – periodic rechecks per Customer policy can be implemented to check for points or disqualification.
Your responsibility:		Provide clear instruction as to when a driving licence check is required. Provide accurate contact information for the candidate.

Ref: PC19	Standard	CIFAS internal fraud database check.
Our responsibility:		Run a candidate's identifying data through the CIFAS internal fraud database and report back on data found.
Your responsibility:		Provide clear instruction as to when CIFAS internal fraud database check is required. Provide accurate contact information for the candidate. Confirm membership of CIFAS and provide their membership number.
Assumptions:		Employers must also be members of CIFAS and provide CIFAS consent for us to run this check.

3 Service Governance

3.1 Service management and reporting

A Customer Success Manager will be allocated to work collaboratively with Customer to ensure a positive service experience. In addition, automated service reporting is provided on a agreed frequency to ensure transparency on service volumes and performance.

3.2 Service Scope

Our Services are based on information supplied by Customer or third parties, the accuracy or completeness of which we cannot guarantee. We use models and techniques based on analytics and probabilities. It is your responsibility to comply with applicable law and to take into account that our Services should not be utilised by Customer as the sole factor in making a business decision but that it is one of many factors upon which Customer should base your decision making. Although we will deliver the Services with reasonable skill and care we cannot accept liability for the said information's accuracy or completeness nor for a failure to achieve a particular result.

3.3 Document Retention

Customer will inform Zellis in writing as to the manner in which Zellis shall perform the Services to comply with data retention requirements during the Term. Additional Charges may apply if your requirements differ from the options available to Customers in

accordance with Zellis' standard data retention policy. If Customer does not provide instructions in writing in accordance with this section, Zellis may implement its standard data retention policy. Further details are available upon request.

4 Audit

4.1 Introduction

We operate within a corporate control framework, encompassing operational, IT, legal and regulatory and security controls that govern our standard business operations. Our dedicated Compliance and Audit management team monitors compliance with our standard control framework and manages our external audits.

Zellis has ISO27001 international standard for information security management systems certification ("ISO27001") at the date of this SDG. Zellis will maintain standards that meet ISO27001 requirements or those of an equivalent certification throughout the term of the Agreement (the "Information Security Standard"). On your request, we will make available to you information on the Information Security Standard that we consider evidences our compliance with the same. If you wish to audit us, such audit will be subject to the terms of this section 4.

4.2 Audit by Customer

Customer may on prior reasonable notice (being not less than (20 Working Days) and at agreed times and intervals (but no more frequently than once in each 12 month period), request to undertake an audit to confirm that the Services comply with the terms of this Agreement (subject to section 4.4).

We will look to agree with Customer the audit method to be employed, based on our methodology and ask that Customer completes our template for audit assistance. Customer will, and will procure that any third-party auditor will, use all reasonable endeavours to organise any audit to minimise any impact on our normal business, including organising audits outside of any payroll calculation week and subject to our required personnel's availability. Audits will be scheduled in accordance with our audit calendar such that no more than two Customer audits will be run concurrently at any one time.

Any third party Customer uses to conduct the foregoing audit should not be a competitor of ours and will be required to execute a confidentiality agreement in advance with confidentiality obligations no less restrictive that those set out in the Agreement.

We will provide Customer and their designated representatives with such co-operation and access to premises, information and Zellis personnel as is reasonably necessary for the audit. In support of your audit rights, we will keep and maintain (i) financial records relating to the Agreement in accordance with international financial reporting standards; (ii) records substantiating our invoices; and (iii) such other records as may be reasonably required for an audit by Customer or a Governmental Authority as permitted within the terms of the Agreement. We will retain the foregoing for the longer of (i) the Term of the Agreement and (ii) as is required by law.

Within a reasonable time (and in any event within ten Business Days) after production of the audit report, we will require Customer to provide us with a copy of the audit report. As soon as reasonably possible after Customer deliver the audit report to us, we will cooperate in good faith to identify and agree upon any appropriate corrective actions and issue any required Change Request Forms.

4.3 Audit by Governmental Authority

If any "Governmental Authority" (being any government department, regulatory authority, judicial or administrative body whether, domestic, international or foreign) conducts an audit of Customer, that includes the Services, we and our Affiliates will, at your request, provide all cooperation and information reasonably required for the purpose of such an audit, (subject to section 4.4) provided that the auditor executes a confidentiality agreement in advance with confidentiality obligations no less restrictive that those set forth in the Agreement.

We will cooperate with any Governmental Authority conducting an audit and provide reasonable access to the premises, equipment, facilities, information and our personnel as is necessary for the audit (provided that such access does not have a material impact on our normal business activities).

4.4 General

Audits carried out will not entitle Customer or a Governmental Authority (including your auditors) to access our internal communications or financial records or to have access to

any element which might put at risk the disclosure of Confidential Information of our other Customers.

Customer to agree that data may be included in our internal monitoring and testing and may be shared with our external auditors across multiple jurisdictions.

We will provide reasonable assistance in support of your audits (including where reasonable, planning and preparation of audits, audit management and reporting meetings, completion of your surveys and questionnaires and face to face meetings). Zellis will not be required to upload information to any Customer nominated portal as part of an audit or conduct any control tests in a live environment.

Together with Customer we will document the scope and timing of the audit as well as the cooperation required of us and the associated costs in a prior written change control note. Audit support provided by Zellis will be charged on a time and materials basis in accordance with Zellis' audit support rate card (as updated from time to time and available on request).

4.5 Cloud Provider Audits

Our Cloud Provider will conduct audits of the security of the computers, computing environment and physical data centres that it uses in processing your data, in accordance with the standards or rules of the regulatory or certification body of and in compliance with the frequency required by the relevant standard or framework.

Each audit will be performed by qualified, independent, third-party security auditors at the Cloud Provider's selection and expense and will result in an audit report, which will available from the Cloud Provider's Audit Site.

The audit report will be the Cloud Provider's Confidential Information and will clearly disclose any material findings by the auditor. The Cloud Provider agrees with us that it will promptly remediate issues raised in the audit report to the satisfaction of the auditor. Customer agrees to exercise your audit right by instructing us to contract with our Cloud Provider to execute the audit as described in this section of the SDG.

Annex A - Digital Right to Work Terms

1. The following terms and conditions apply to Digital Right to Work services ("**DRtW Services**"):

(a) The Customer represents and warrants that:

(i) it is located in the United Kingdom and it will only access the DRtW Services and related materials in the United Kingdom;

(ii) it will use the DRtW Services in accordance with applicable Law;

(iii) it will only use the DRtW Services for internal business purposes for itself and for the benefit of its Affiliates;

(iv) it will be responsible for providing required notices and gaining required consents, authorisations or securing the lawful basis for processing under DP Law;

(v) it will not use the DRtW Services or related materials for the following purposes: (A) claims management; (B) credit assessment; (C) investigative journalism; or (D) marketing;

(vi) it has not been subject to enforcement action by the Information Commissioner's Office ("**ICO**") or the Financial Conduct Authority;

(vii) it is not known or suspected to have been involved in credit fraud or other unethical business practices (either by the Customer itself or by an individual affiliated with the Customer);

(viii) it is not known or suspected to be engaged in fraudulent or illegal activity, such as identity theft, harassment or stalking;

(ix) it is not listed on the OFAC's list of Specially Designated Nationals, the UK's HM Treasury's Consolidated List of Sanctions Targets, or the EU's Consolidated List of Persons, Groups, and Entities Subject to EU Financial Sanctions; and

(x) it has a data protection number and an active registration with the ICO unless the Customer is exempt under applicable Law as it is a non-profit or central or local government entity.

(b) If Zellis reasonably believes that the Customer is in breach of section 1(a) of this Annex, Zellis may withhold the provision of the DRtW Services until such time that

Zellis is satisfied that the Customer is compliant with all representations and warranties.

(c) Zellis and its subcontractors may retain and share with the Metropolitan Police, other UK law enforcement authorities and regulatory bodies (together "**Authorities**") any data in relation to fraudulent documents where reasonably required by such Authorities for the purposes of fraud prevention, such right to continue after termination of this Agreement.

(d) Unless expressly agreed in writing to the contrary, Zellis and its subcontractors may retain the name and address of subjects of checks for up to and including six years (to allow Zellis and its subcontractors to defend any legal claims in respect of such checks).

(e) The Customer accepts responsibility for the selection of the DRtW Services and the extent of the DRtW Services as set out in this Service Description Guide to achieve its intended results and acknowledges that the DRtW Services have not been developed to meet the individual requirements of the Customer.

(f) The Customer acknowledges that the following permitted purposes apply to the following elements of the DRtW Services:

(i) **Death Registry Information (DRI) Data:** Customers are granted access to this data for the primary purpose of prevention, detection, investigation and prosecution of offences. Customers shall not access or permit anyone to access the DRtW Services in respect of Death Registration Information from a country outside the UK, nor export or permit the export of data or results comprising Death Registration Information to a country outside the United Kingdom.

(ii) **Equifax Consumer Credit Header Data:** Customers are granted access to this dataset for the purpose of:

(A) assisting in the prevention of money laundering;

(B) ID verification; and

(C) detecting fraud in relation to the granting of credit to consumers.

For further information please visit zellis.com

A4190/MCB29 November 2024
Zellis Background Checking Services Description - v1_2 FINAL.docx