

veremark.



How To Ensure Your SMCR-Based Criminal Background Checks Comply with GDPR

Table of

Contents

Executive Summary	3
How To Ensure Your SMCR-Based Criminal Background Checks Comply with GDPR	4
1. Establish if SMCR applies	5
2. Establish your SMCR category	5
3. Understand where General Data Protection Legislation (GDPR) Impacts SMCR	5
4. Establish Valid GDPR Justification For Background Checking	6
5. Perform a Data Protection Impact Assessment (DPIA)	7
6. Create a Data Protection Policy	7
7. Update the 'records of processing'	8
Sticky Wicket	8
Checklist and Action Plan	9
Veremark SMCR Employer Compliance Package	10
Contacts	11

Executive Summary


On 9th December 2019, the Senior Managers and Certification Regime (SMCR) was extended to cover solo-regulated firms. From this date, around 50,000 asset managers, brokers and consumer credit firms will be required by law to conduct criminal background checks on specified staff.

The new screening regime must be carefully implemented to ensure compliance with the General Data Protection Regulation (GDPR). This efficient 7-point guide outlines how to conduct SMCR-Based criminal background checks while complying with GDPR.

Readers will learn the 'legal bases' and 'valid conditions' criteria of General Data Protection Legislation (GDPR) and UK Data Protection Act (DPA), which must be fulfilled before organizations can legally conduct criminal background checks.

The guide also outlines the full due process that must be followed to do GDPR compliant criminal background checks, including:

1. Establishing adequate legal basis,
2. Perform a Data Protection Impact Assessment (DPIA)
3. Creating a Data Protection Policy
4. Updating Records of Processing



The report ends with a 9-point check-list and action plan for employers.

How To Ensure Your SMCR-Based Criminal Background Checks Comply with GDPR

On 9th December 2019, the Senior Managers and Certification Regime (SMCR) will be extended to cover all solo-regulated firms. This means that around 50,000 asset managers, brokers and consumer credit firms will fall under the Financial Conduct Authority's (FCA), new enhanced background checking regime.

The implementation of the SMCR is complicated by the fact that complying with this regime requires a criminal history background check,

which can only be done after satisfying specific requirements of prevailing data protection legislation.

We have prepared a guide on how to implement SMCR criminal background checking, while complying with data protection laws.



1. Establish if SMCR applies

As you'll probably know, SMCR was introduced to banking firms in 2016 and insurers in 2018. If you are a solo-regulated firm SMCR will [apply to you from December 2019](#).

2. Establish your SMCR category

It's important to [establish your SMCR category](#) from the Financial Conduct Authority (FCA) site, as the compliance burden is proportionate to the size of the firm. The three categories are, 'Limited Scope, Core and Enhanced' and the administrative load increases with each category.

In reality, with the deadline drawing close, most solo-regulated firms should be well along the way to December 2019 SMCR compliance. It's the associated step, where the SMCR collides with data protection legislation which many of you may still be wrestling with, or even unaware of.



3. Understand where General Data Protection Legislation (GDPR) Impacts SMCR

The SMCR regulation requires that, from December 2019, solo-regulated organizations do more stringent background checking of individuals applying for, or currently performing Certified or Senior Manager roles, to check that they are fit and proper to perform their jobs. The background checks assess fitness and propriety, by examining the honesty and integrity of relevant candidates or job holders.

Where SMCR overlaps with the data protection regulation is that organizations are required to establish whether the individual has a criminal record, which is an information category carefully controlled by data protection laws. This means that in doing nothing more than complying with SMCR, organizations could breach data protection laws, and there-in lies the conflict.

Therefore, if a firm wants to process criminal records data, it must establish 'legal bases' under General Data Protection Legislation (GDPR) and a valid condition under the UK Data Protection Act (DPA) before doing so. Failure to comply with GDPR can lead to fines of up to €20 million or 4% annual global turnover, whichever is higher.

4. Establish Valid GDPR Justification For Background Checking

The immediate question is whether the SMCR requirement for criminal background checking gives firms the 'legal basis' under GDPR and a valid 'condition' under the DPA to perform this check. The good news is that it does but only for senior managers for which criminal background checks are mandatory under FCA regulation. This legal base justification for criminal background checks doesn't automatically extend to the second category of worker covered under the SMCR regime, that is the 'Certified Person'. This is because criminal background checks for Certified Person's are deemed optional by SMCR not mandatory, which means that firms can't rely on SMCR as a legal basis for doing criminal background checks.

Does this mean that firms can not perform criminal background checks on Certified Persons due to GDPR and DPA restrictions? No, such checks can still be performed, but you need to use alternative justification to complete these criminal background checks legally, and these are:

- It's in the firm's legitimate interest
- It's done with the individual's consent
- There are caveats around using this justification for certified persons such as:
- Firms cannot require such candidates to provide detail on spent convictions under the Rehabilitation
- of Offenders Act 1974
- Legitimate interest must be balanced with the person's privacy rights and evidence
- There are question marks around whether employees and candidates can validly give consent due to the employer holding a favourable balance of power.

In order to comply with the SMCR requirement for increased background checking without falling foul of data protection you may need to make some changes to your data management practices which are explained below.

5. Perform a Data Protection Impact Assessment (DPIA)

When processing any new form of data likely to result in high risk for individuals you are required to carry out a [Data Protection Impact Assessment DPIA](#). This risk assessment will enable you to identify and minimise risks of doing criminal background checking under SMCR. Your DPIA must

- describe the nature, scope, context and purposes of the processing;
- assess necessity, proportionality and compliance measures;
- identify and assess risks to individuals; and
- identify any additional measures to mitigate those risks.

6. Create a Data Protection Policy

Having completed your impact assessment, data protection law dictates that you create a policy explaining how you'll process criminal records, and this should include sections on

- Information security practices, process, technology and how this high risk data will be kept secure
- and safe from theft, and how long you'll retain the data for
- Upholding subject right, relating to accessing data, modifying data



7. Update the 'records of processing'

By now, you should already have a 'records of processing' as this is a requirement for all organizations handling [personal data since GDPR came into force](#) a few years back. If you don't have one, you'll need to establish one as there are significant fines for not properly maintaining one. You can read more about this [here](#) at the GDPR's home site.

Since you are adding criminal background checking to your data processing regime you'll need to update your 'records of processing' to reflect this.

Specifically you'll need to document the type of data you'll be processing, the data subjects, (certified persons and senior managers), why you are processing it, (SMCR) and the data recipients, (your firm, FCA).

You'll also need to set out the legal bases and conditions that are relying on for legitimately processing this data.

Sticky Wicket

There are two potentially thorny areas that need further consideration. Since criminal background checking is not a mandatory requirement for certified persons you don't have a valid legal basis under GDPR to do a criminal background check. If you do want to do a criminal check on this category of worker, you'll need to rely on conditions which rely on some degree of interpretation.

As a result of this, it would be prudent to consult a data protection lawyer before going down this particular route.

Checklist and Action Plan

There is a lot to take in here and so we have developed a simple checklist of items to help you develop an action plan for change.

1. Establish if SMCR applies to your organization before proceeding as compliance is a serious undertaking. This is good page to read: <https://www.fca.org.uk/publications/policy-statements/ps19-20-optimising-senior-managers-certification-regime-and-feedback-cp19-4>
2. Establish which SMCR category your organization falls under as this determines your compliance workload and key tasks, and will enable you to develop your compliance-road-map. This is a good page to read: <https://www.fca.org.uk/firms/senior-managers-certification-regime/solo-regulated-firms>
3. Establish a project team and executive sponsor (to ensure traction) as soon as possible. Ensure project team members are allowed time, budget and resources to achieve their goals.
4. Identify your Senior Managers and Certified Persons under SMCR regulations
5. Establish the GDPR-compliant legal basis for criminal background-checking under SMCR
6. Prepare a Data Protection Impact Assessment, (DPIA). You can download a DPIA Assessment Template Here: <https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf>
7. Create a GDPR policy explaining how you'll process criminal background check data.
8. Update the records of processing
9. Have your plan vetted by a legal or compliance professional

Not SMCR Compliant Yet? We can Help!



Veremark SMCR Employer Compliance Package £200

- FCA regulated (Senior Manager Regime)
- UK Online Identity Check
- UK Criminal Record (Standard)
- Last 6 Years of Activity References
- UK Credit Check
- International Fraud / Sanctions Search
- UK Investigative Directorship Check
- Highest Level of Educational Qualification
- Professional Qualification/Membership
- Passport Validation
- FCA References (when applicable)
- Financial Services Register Check
- CV Comparison



veremark.com

London

85 Great Portland Street London, England,
W1W 7LT, United Kingdom

Manila

Unit 3 Ground Floor CTP Alpha Tower,
Investment Drive Madrigal Business Center
Ayala Alabang Muntinlupa City,
Philippines 177

Singapore

30th Floor, Singapore Land Tower,
Raffles Place, Singapore

Contact Us

dan@veremark.com