



Department  
for Business  
Innovation & Skills

**TRANSPARENCY AND TRUST:  
ENHANCING THE TRANSPARENCY  
OF UK COMPANY OWNERSHIP AND  
INCREASING TRUST IN UK  
BUSINESS**

**PRIVACY IMPACT ASSESSMENTS**

**JUNE 2014**

# Contents

<b>Introduction .....</b>	<b>3</b>
<b>Company Beneficial Ownership: Privacy Impact Assessment .....</b>	<b>5</b>
Annex A: Privacy impact assessment screening questions.....	15
Annex B: Identification of Risks .....	21
Annex C: Linking the guidance to the Data Protection principles .....	25
<b>Bearer Shares: Privacy Impact Assessment .....</b>	<b>35</b>
Annex A: Screening process for a small scale PIA .....	40
Annex B: Screening process for a full scale PIA.....	44
<b>Company Directors: Privacy Impact Assessment .....</b>	<b>47</b>
Annex A: Screening process for a small scale PIA .....	53
Annex B: Screening process for a full scale PIA.....	57
<b>Director Disqualification: Privacy Impact Assessment .....</b>	<b>61</b>
Annex A: Screening process for a small scale PIA .....	72
Annex B: Screening process for a full scale PIA.....	75

# Introduction

1. The following document includes the Privacy Impact Assessments (PIAs) for measures included in Part 7 ('Companies: Transparency') and Part 9 ('Directors' Disqualification etc.') of the Small Business, Enterprise and Employment (SBEE) Bill ('Companies: Transparency').
2. Privacy screening processes have been carried out for the following measures:
  - a. Enhanced Transparency of Company Beneficial Ownership<sup>1</sup>
  - b. Prohibiting Bearer Shares in UK Companies
  - c. Company directors
  - d. Director disqualification
3. With the exception of the company beneficial ownership measure, the screening processes found that full PIAs were not required. A full PIA has been carried out for the company beneficial ownership measure and is included below.

## Background

4. A lack of transparency and of accountability with respect to those controlling a company can facilitate illicit activity, erode trust and damage the business environment. Ultimately this can hold back economic growth.
5. The UK has put corporate transparency on the international agenda. At the Lough Erne G8 Summit in June 2013, the Prime Minister led the G8 countries in agreeing to a number of core Principles to prevent the misuse of companies and legal arrangements.
6. The Department for Business, Innovation and Skills (BIS) subsequently published the Transparency and Trust discussion paper (July 2013). In it we sought views on how to improve corporate transparency and accountability in the UK. This included how best to proceed with the corporate transparency proposals in the UK's 2013 G8 Action Plan, and a range of related measures to improve confidence in the UK's regime for tackling company directors who have engaged in misconduct.

---

<sup>1</sup> Provision for the central registry of company beneficial ownership information is referred to in the SBEE Bill as 'a register of people with significant control'.

7. On the 21 April 2014 BIS published the Government's response to the views received in relation to the Transparency and Trust discussion paper. The response set out how we intended to take forward reform. Provision has accordingly been made in the SBEE Bill, which was introduced into Parliament on 25 June 2014.

## Privacy Impact Assessments

8. The PIAs in this document have been conducted in order to identify any data protection issues in relation to the various sections of the Transparency and Trust package. The PIAs have identified any potential privacy risks and focus on ensuring that the policy complies with the Data Protection Act 1998 (DPA) and other relevant legislation.
9. The purpose of the PIA is to minimise privacy risks while meeting the aims of the project. Whilst conducting a PIA is not a legal requirement of the DPA, it is beneficial to identify any privacy risks relating to the policies.
10. The documents will be updated in light of any changes made to the policy which may have an impact on privacy, particularly in the context of the measure on company beneficial ownership. The PIAs below are current as of June 2014.
11. Please contact the Transparency and Trust team at the Department for Business, Innovation and Skills ([transparencyandtrust@bis.gsi.gov.uk](mailto:transparencyandtrust@bis.gsi.gov.uk)) if you require more information.

# Company Beneficial Ownership: Privacy Impact Assessment

## The issues and goals of the policy

1. Company records (held by the company and at Companies House) provide information about a company's directors and members ("shareholders"). But companies are not currently required to provide information about the individuals who ultimately own and control the company - the 'beneficial owners' or 'people with significant control'.
2. Companies can be used as a front to facilitate crime, from money laundering and terrorist financing to tax evasion and drug trafficking. Elaborate and opaque ownership structures to obscure the beneficial ownership of a company can play a part in this.
3. Our Final Stage Impact Assessment (published separately) set out the estimated scale of UK and global illicit financial flows, and the way this links to the misuse of companies generally, and beneficial ownership in particular.
4. This problem was recognised by the G8 during the UK's Presidency in 2013. As a result, G8 members agreed a set of common principles to tackle the misuse of companies and legal arrangements<sup>2</sup>. Each G8 member published an Action Plan setting out how they would implement these principles. In that context the UK committed to implement a **publicly accessible central registry of company beneficial ownership information**<sup>3</sup>.

## What does the policy set out to achieve?

5. The policy will require UK companies to obtain and hold adequate, accurate and current information on their beneficial ownership. A beneficial owner is any individual who ultimately owns or controls more than 25% of a company's shares or voting rights, or who otherwise exercises control over the company or its management. This information will be publicly accessible onshore in a central registry maintained by Companies House. The registry will provide a single

---

<sup>2</sup> G8 (June 2013): <https://www.gov.uk/government/publications/g8-action-plan-principles-to-prevent-the-misuse-of-companies-and-legal-arrangements/g8-action-plan-principles-to-prevent-the-misuse-of-companies-and-legal-arrangements>

<sup>3</sup> G8 (June 2013): <https://www.gov.uk/government/publications/uk-action-plan-to-prevent-misuse-of-companies-and-legal-arrangements/uk-action-plan-to-prevent-misuse-of-companies-and-legal-arrangements> and Open Government

source of information to support national and overseas law enforcement and tax authorities' investigations; support financial institutions and other regulated professional bodies as they carry out anti-money laundering due diligence checks on companies; and allow all those who engage with a company (e.g. investors, suppliers, customers) to identify with whom they are really doing business. The overarching policy objectives are to reduce crime and improve the business environment so as to facilitate economic growth. The UK has determined that these policy objectives can be best served through greater transparency (i.e. by making information publicly accessible).

6. The policy should also:

- Stimulate global, collective action to tackle the misuse of companies. Investigations into abuses of company structures will often cross borders and so coordinated international action is vital. In leading by example, UK and G7 action should encourage other jurisdictions, including the UK's Overseas Territories and Crown Dependencies, to follow suit. This should deliver better outcomes in terms of reducing crime in the UK as well as elsewhere;
- Deliver benefits for developing countries who suffer as a result of tax evasion, corruption and fraud. By allowing them access to information on UK companies, they should be more easily able to identify the individuals really responsible where a UK corporate entity has been used to facilitate the crime; and
- Ensure full UK compliance with relevant international standards in advance of the UK's next Financial Action Task Force (FATF) peer review in 2016 to maintain and enhance the UK's reputation as a clean and trusted place to do business and invest.

## Who is likely to be affected by this policy?

7. This policy will primarily impact UK companies and the beneficial owners of those companies. A wider population may derive benefits from the policy as a result of reduced crime or an improved business environment.
8. The FAME database reports that there are **3.24m UK companies**<sup>4</sup>. This figure includes active and dormant companies, and companies in the process of being dissolved. This figure also includes Limited Liability Partnerships (LLPs).

---

Partnership (October 2013): <https://www.gov.uk/government/speeches/pm-speech-at-open-government-partnership-2013>

<sup>4</sup> Company population estimates were extracted from the FAME database (Bureau Van Dijk Electronic Publishing, 2013). This figure includes Limited Liability Partnerships (LLPs). For the purpose of this document, the term 'companies' will include LLPs.

9. The proposed policy exempts companies with securities listed on a UK regulated or prescribed market<sup>5</sup>, as they are already subject to stringent ownership disclosure requirements, and those on a non-UK market subject to equivalent disclosure requirements. We would also intend to exempt Limited Partnerships, European Economic Interest Groupings, industrial/provident companies and overseas companies. Applying these exemptions to the FAME population gives an estimated number of companies in scope of **3,185,000**.
10. The number of beneficial owners is currently unknown. Companies House indicate that 1.5m companies have one shareholder and 2.96m have fewer than four shareholders. It is plausible that on average companies will have two shareholders. If we assume that the number of shareholders is a proxy<sup>6</sup> for the number of beneficial owners then on average companies might have two beneficial owners. However, some companies will not have any beneficial owners and others might have more than three, e.g. where the beneficial owners are acting jointly to own or control the company. Furthermore some individuals will be beneficial owners of more than one company. On this basis it is not possible to estimate reliably the number of beneficial owners.
11. The existing definition of beneficial ownership, as applied in the anti-money laundering context, will be used as the basis for our statutory definition of 'beneficial ownership' in the context of these new requirements. This means that information on individuals who ultimately own or control more than 25% of a company's shares or voting rights, or who otherwise exercise control over the company or its management, will need to be obtained and held by the company and provided to the central registry. Where a qualifying beneficial interest in a company is held through a trust arrangement, the trustee(s) or any other individual(s) exercising effective control over the activities of the trust will be required to be disclosed as the beneficial owner of the company.
12. We intend to place an obligation on both companies and individuals to identify and obtain information on beneficial ownership. Companies will be required to take reasonable steps to identify their beneficial owners. They will be given statutory tools to help them obtain this information, including the ability to serve notice on a person (as specified in the legislation) to obtain information. Individuals will be required to disclose this information to the company, unless it is already held by the company.

---

<sup>5</sup> Australian Securities Exchange, Boerse Berlin, Boerse Frankfurt, Bolsa de Madrid, Bursa Malaysia, Channel Islands Stock Exchange, Euronext Amsterdam, Euronext Brussels, Euronext Paris, GXG Regulated Market, Hong Kong Stock Exchange, ICAP Securities & Derivatives Exchange (ISDX), Irish Stock Exchange, Johannesburg Stock Exchange, London Stock Exchange, London Stock Exchange (SEAQ), NASDAQ Dubai, NASDAQ National Market, Nasdaq OMX – Helsinki, Nasdaq OMX – Stockholm, New York Stock Exchange, Norwegian OTC, Oslo Bors, Oslo Bors, OTC Bulletin Board, OTC Pink Market, Other OTC Market, USA, Swiss Exchange, Tokyo Stock Exchange, Toronto Stock Exchange, TSX Venture Exchange, Warsaw Stock Exchange, Wiener Boerse, XETRA.

<sup>6</sup> The number of legal shareholders is not synonymous with beneficial owners, however, robust data on the latter is not available.

## What data will be collected and published? How will this be done?

13. Companies will be required to maintain a register of beneficial owners (referred to in the draft legislation as a 'register of people with significant control'). This will contain information on the beneficial owners' full name, date of birth, nationality, country or state of usual residence, residential address, service address, date on which they acquired control over the company and details of the nature of that control.
14. This data does not constitute sensitive personal data under the Data Protection Act 1998 (DPA). This register will be kept available for public inspection via the company, with the exception of residential addresses.
15. Companies will be required to update the information held in their register of beneficial owners if they know or might reasonably be expected to have known that a change to their beneficial ownership has occurred. Beneficial owners will be required to inform the company of any changes to the information recorded in the register of beneficial owners.
16. All of the information held by the company will be provided by the company to Companies House. It will be accessible publicly at Companies House with the exception of residential addresses and full dates of birth. This is consistent with the position in respect of company directors' residential addresses, and the new policy arising out of the Company Filing Requirements consultation to suppress the 'day' of the date of the birth on the public register to assuage identity theft and data privacy concerns<sup>7</sup>. The month and year of birth will remain on the public record.
17. We intend to allow applications to the registrar of companies (Companies House) to protect beneficial owners' full information from public disclosure in exceptional circumstances. Information withheld from public inspection is referred to as 'protected information'. Specified UK and overseas enforcement authorities will be able to access protected information held at Companies House, provided we can be satisfied that data shared in this way will be used and stored appropriately. We are currently working through a number of options as to how the UK might achieve this objective, including looking closely at whether it would be appropriate to follow existing models for information exchange.
18. Companies will be required to provide an initial statement of beneficial ownership on incorporation. They will not be registered at Companies House unless this information is provided. Companies will then be required to confirm that the

---

<sup>7</sup> Unless the company opts to maintain its beneficial ownership register at Companies House, in which case the full date of birth will be publicly available.



information held at Companies House is correct at least once every 12 months, detailing all changes that have occurred in-year.

19. We want however to ensure companies can update this information as it changes should they wish to do so, in the interests of maximum transparency. That is why complementary proposals in the Company Filing Requirements package of reform will enable companies to update the information held at Companies House more frequently. In addition, private companies will be able to hold and update their register of beneficial ownership at Companies House directly should they wish to do so. Should they choose to exercise this option, they would need to update the information held at Companies House as they become aware of changes (in the same way that they would otherwise be required to update their own beneficial ownership register).
20. We will extend or replicate existing company law criminal offences to tackle situations where companies or individuals break the rules.
21. The introduction of a central registry of company beneficial ownership information is a significant and complex reform, requiring both primary and secondary legislation. It will be important that we provide sufficient flexibility in primary legislation to allow us to keep the policy under review in the light of experience and changing circumstances. We will therefore place a statutory duty on the Secretary of State to publish a review of the efficacy and proportionality of the registry within three years of implementation.

### ***Data retention***

22. To comply with the 5th Principle of the Data Protection Act 1998 (DPA), personal data should not be kept for longer than is required for the purpose for which it has been acquired.
23. Information is delivered to the registrar under statute. Companies House is therefore exempt under section 34 of the DPA from the majority of the Data Protection Principles. The Companies Act 2006 requires the registrar to make the information available for public inspection including the right to a copy (see section 1085 and section 1086) except in certain cases (see for example section 240 and section 1087).
24. Section 34 of the DPA states:

*“Information available to the public by or under enactment.*

*Personal data are exempt from—*

*(a) the subject information provisions,*

*(b) the fourth data protection principle and section 14(1) to (3), and*

(c) *the non-disclosure provisions,*

*If the data consist of information which the data controller is obliged by or under any enactment [other than an enactment contained in the Freedom of Information Act 2000] to make available to the public, whether by publishing it, by making it available for inspection, or otherwise and whether gratuitously or on payment of a fee<sup>8</sup>.*"

25. Further information on subject information provisions and non-disclosure provisions can be found on the [Information Commissioner's Office website](#).
26. Data will remain on the company's register for 10 years after the date on which a person ceases to be a beneficial owner. This is consistent with the retention period that applies currently in respect of company shareholders.
27. Data will remain on the register at Companies House indefinitely unless the company is dissolved. In that case the registrar may direct the records to the Public Record Office a minimum of two years after the dissolution. Beyond this there is no need to consider retention because of the general exemption from the 5th Principle.

### **Data transfer**

#### *Public register*

28. The 8th Principle provides that data must not be transferred outside the European Economic Area (EEA) unless adequate levels of protection are in place in relation to the processing of personal data.
29. However, data on the public register is exempt from the 8th Principle by virtue of Schedule 4 to the DPA. Schedule 4 outlines cases where the 8th Principle does not apply. Paragraph 7 of Schedule 4 states contains an exemption for a transfer that is part of the personal data on a public register: *"The transfer is part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data are or may be disclosed after the transfer."*
30. In terms of data transfer, information on the public register will therefore be held, used and disclosed in line with the provisions of the Companies Act 2006 and the DPA, where applicable.

---

<sup>8</sup> <http://www.legislation.gov.uk/ukpga/1998/29/section/34>

*Private register*

31. We are carefully considering which UK and overseas authorities should be allowed access to the private register and how. In this case, we use 'private register' to refer to information held by Companies House which is not made available publicly, namely residential addresses, full dates of birth and information on individuals whose data is to be withheld from public inspection. We are giving particular consideration to how overseas authorities can access this information quickly and easily, whilst also ensuring that any information shared is appropriately used and stored.
32. This element of the policy will be set out in secondary legislation and we intend to further seek wider stakeholder views on this. Proposed options will take full account of the Data Protection Principles and we will update the PIA as necessary.

**External consultation**

33. BIS published the [Transparency and Trust: Enhancing the transparency of UK company ownership and increasing trust in UK business discussion paper](#) in July 2013. This document asked stakeholders and the general public for their views on the *Transparency and Trust* proposals set out within the document.
34. The views received in response to that discussion paper have informed our current policy, including in relation to the information to be collected and made publicly available and any exemptions regime that should apply.
35. We have also engaged with numerous stakeholders on beneficial ownership, as part of our comprehensive stakeholder engagement strategy. These have included representatives from the legal, accounting and banking professions; business representatives; civil society organisations and law enforcement agencies. During these meetings we have discussed, amongst other issues:
- The definition of 'beneficial owner';
  - The data to be collected and made available publicly, including possible risks and options to mitigate those risks;
  - The sharing of data – both nationally and internationally; and
  - The protection of individuals at risk.
36. We have also discussed our proposals with the Information Commissioner's Office (ICO) and the IDAP Privacy and Consumer Advisory Group, focussing specifically on privacy considerations. These discussions have not raised particular concerns in relation to the policy.

37. We published the [Transparency and Trust: Enhancing the transparency of UK company ownership and increasing trust in UK business government response](#) in April 2014, outlining the policies and proposals we plan to take forward. This document again invites stakeholders to provide opinions on aspects of the beneficial ownership policy, primarily around the definition of beneficial ownership, exemptions, obtaining the information, the information to be collected and who this data should be shared with.
38. We will continue to engage with a wide range of stakeholders as we further develop and refine our policy. This will be particularly important in the context of the development of the protection regime for beneficial owners who may be put at risk as a result of public disclosure of their personal information; and in the context of sharing information on the private register with national and international authorities.

### ***Internal consultation***

39. The BIS Transparency and Trust team have engaged with Legal, Information and Technology directorate, Companies House and the Insolvency Service in conducting this PIA.

## **Why is a PIA needed?**

40. Key reasons from screening process why a PIA is needed:
- Collection of new information about individuals;
  - Information about individuals being disclosed to organisations or people who have not previously had routine access to the information; and
  - Using information about individuals for a purpose it is not currently used for, or in a way it is not currently used.
41. The need to complete a privacy impact assessment (PIA) was informed by the completion of the PIA screening process, as outlined in the ICO guidance on Conducting Privacy Impact Assessments Code of Practice. This completed screening process for the central registry can be found in **Annex A** below.

### ***Identification of Privacy Risks***

42. In addition to the screening process outlined in **Annex A** below, we have identified and recorded privacy risks.
43. The tables in **Annex B** show these risks, as well as our proposed solutions. These risks will be kept under review over the lifetime of the project and the tables will be updated as necessary.

### ***Data Protection Principles***

44. In addition to the above, we have identified where our policy will fit in with the Data Protection Act Principles. This analysis is outlined below in **Annex C**.

## **Signing off the PIA outcomes**

45. The analysis above clearly shows the risks involved in establishing a central registry of company beneficial ownership information. We are confident that those risks identified have been sufficiently mitigated to an appropriate level, minimising the impact that the policy will have on the following areas:

- Public harassment
- Identity theft
- Fraud or other serious crime
- Intrusiveness

46. Our policy around the following is still being developed:

- Misuse by overseas countries
- Overseas countries systems are insufficiently secure (e.g. can be hacked into) leading to inappropriate use or transfers of data
- Protection of information on vulnerable persons

47. Given that the policy around sharing the information with overseas agencies and the protection regime is still being developed, we have not sought to quantify this risk at this stage. However, as noted, we will ensure that this information is shared appropriately and in line with the Data Protection Principles. We will update the PIA as appropriate as the policy is developed.

48. We are continuing to engage with stakeholders on a number of issues around the register and there are areas where our thinking continues to develop. We are committed to ensuring that any changes comply with the DPA and have minimal impact on the privacy of individuals.

## **Integrating the PIA outcomes back into the project plan**

49. As noted above, any changes to the policy may require risk solutions to be reconsidered. If this is the case, we will update this document to reflect the new

policy, identify the associated risks and outline how we have planned to mitigate this risk. We will also link these policy changes to the DPA to ensure full compliance. The PIA will be kept as a working document to reflect any changes in the policy.

50. Implementing a central registry of company beneficial ownership information is a significant and complex reform. Reform will require primary amendments to the Companies Act 2006. Provision for this is made in the Small Business, Employment and Enterprise (SBEE) Bill.
51. As is usual in company law, we will look to implement the policy detail through secondary legislation. We will look to do this as soon as practicable after the primary legislation has received Royal Assent. We will then look to implement the registry as soon as practicable once all primary and secondary legislation is in place. In implementing reform we will carefully consider the transitional arrangements that will be required for existing companies.

## Conclusion

52. We are confident that this Privacy Impact Analysis accurately reflects the privacy risks associated with the beneficial ownership policy. We are satisfied that these risks have been mitigated to an appropriate level, in accordance with the Data Protection Act 1998. We will keep this document under review as elements of the policy are further refined, and update it as necessary.
53. In addition, the Bill seeks to place a statutory duty on the Secretary of State to publish a review of the efficacy and proportionality of the central registry within three years of implementation. This should include consultation. This will provide an opportunity to reconsider any particular privacy issues associated with the policy.

## Annex A: Privacy impact assessment screening questions

### 1. Will the project involve the collection of new information about individuals?

Yes.

The identifiers currently required to be held by the company and provided to Companies House for an individual company director are set out in the Companies Act 2006 and include:

- any name and former name
- a service address
- country of residence
- nationality
- occupation
- date of birth<sup>9</sup>
- residential address – not on the public record at Companies House or made available publicly by the company

#### ***Impact on beneficial owners of UK companies***

The register will hold information on the individuals who ultimately own and control UK companies, whether by ultimately owning or controlling more than 25% of the company's shares or voting rights, or by otherwise exercising control over the company or its management.

Under the new proposal, the following information about the beneficial owner will need to be held by the company and provided to Companies House:

- full name;
- date of birth;
- nationality;

---

<sup>9</sup> Other measures in the SBEE Bill will alter the current requirement for a full date of birth to be made available publicly at Companies House in respect of directors (and beneficial owners). The month and year of birth only will be on the public record at Companies House *unless* the company has opted to maintain its register of directors at Companies House (again under reforms proposed in the SBEE Bill).

- country or state of usual residence;
- residential address;
- a service address;
- the date on which the beneficial owner acquired the beneficial interest (and ceased to hold it, where applicable); and
- details of the individual's control over the company.

As for directors, the full date of birth will not be available on the public record at Companies House. The residential address will not be available either via the company or Companies House other than to specified authorities.

There is currently no information held centrally or routinely by Government on individuals who are the beneficial owners of UK companies. Some beneficial owners will be company directors or shareholders. The extent to which this policy collects new information therefore depends on the beneficial owner and whether they have provided their details to Companies House previously. Information on many beneficial owners of UK companies will already be held by regulated professional bodies such as banks, lawyers and accountants (under the Money Laundering Regulations 2007). It is not however clear to what extent the information they hold on beneficial owners mirrors that which we intend to collect; and this information would not be publicly available.

## **2. Will the project compel individuals to provide information about themselves?**

**Yes.**

Under our proposals, UK companies will be required to obtain and hold information on their beneficial owners and provide this to a publicly accessible central registry maintained by Companies House. Information may be collected by the company by way of notice served on the individual, or other means. The company will not be able to enter information in their register (and therefore, this will not be provided to Companies House) unless it has been provided by the individual or by a person authorised to act on behalf of the individual.

Individuals will also be required to disclose their beneficial interest in the company to the company (unless the company already has this information).

We do intend to allow individuals (and likely also companies on their behalf) to apply for an exemption from public disclosure where they consider themselves at serious risk of harm (and possibly also other criteria).



**3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?**

**Yes.**

Given that the proposal involves the collection and publication of new information about individuals, organisations and people will have access to information which they did not previously have.

Access arrangements to the company's own register will replicate those currently in place for inspection of information on company shareholders. Information held by Companies House will be publicly accessible with the exception of full dates of birth, residential addresses and information on individuals at risk of serious harm which has been protected from public disclosure.

As an example of how this information will be used, NGOs intend to use the information to support their investigations into corruption, money laundering and other criminal activities. Law enforcement agencies will use the registry to support their investigations – it will provide an additional source of intelligence to identify criminality and provide evidence to be used in criminal proceedings. Those that engage with companies (e.g. suppliers and investors) may use the information to identify who ultimately owns and controls the companies with which they are doing business; and banks and other regulated professions may use the information to support their anti-money laundering due diligence checks into potential clients.

We are carefully considering which UK and overseas authorities should be allowed access to the private register and how. We are giving particular consideration to how overseas authorities can access this information quickly and easily, whilst also ensuring that any information shared is appropriately used and stored.

**4. Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?**

**Yes (and see above).**

This information will already be being collected by regulated professional bodies (and see above) for the purpose of anti-money laundering due diligence checks; and law enforcement agencies will already be using this information, where it is available, for the purpose of criminal investigations.

However, making this information publicly and centrally available via companies and Companies House means that the information could in future be used for a wider range of purposes. For example, to build a picture of a business in the context of company transactions or credit decisions.

**5. Does the project involve you using new technology that might be perceived as being privacy intrusive? For example, the use of biometrics or facial recognition.**

**No.**

**6. Will the project result in you making decisions or taking action against individuals in ways that can have a significant impact on them?**

**Yes.**

Criminal penalties will be used to tackle individuals and companies that break the rules because we are serious about implementing a strong compliance regime. Indeed, tackling crime is one of the core policy objections for this project.

This means that the non-provision or false provision of information by individuals or companies could ultimately result in a criminal sanction, including imprisonment in some cases.

In addition, it is likely that the exemptions regime will result in Government, or public sector agencies, making decisions about whether an individual's information should or should not be made available publicly based on applications submitted. If Government were to decide against the application, this could arguably have a significant impact on that individual (if indeed the person were, for example, at serious risk of harm).

**7. Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be private.**

**No.**

Individuals identified as beneficial owners will be required to provide Companies House with the information outlined below:

- full name;
- date of birth;
- nationality;
- country or state of usual residence;
- residential address;
- a service address;

- the date on which the beneficial owner acquired the beneficial interest (and ceased to hold it, where applicable); and
- details of the individual's control over the company.

While this may constitute a considerable amount of personal data, the information requested is not significantly different from the data currently collected by Companies House on company directors. In this context, this data can be considered proportionate, particularly given the objective of the policy which is to ensure that individuals can be uniquely identified in the vast majority of cases from information on the public register alone.

As mentioned above, the 'day' of the date of birth will be redacted from the public register (unless the company has opted to maintain its beneficial ownership register at Companies House), and residential addresses and full dates of birth will only be accessible by specified authorities.

The publication of individuals' names and service addresses in a central register may increase the risk of public harassment or other criminal activity such as fraud. However, much of this information will already be in the public domain (e.g. through information on the electoral roll or where the beneficial owner is also a company director). We have also taken steps to mitigate this, e.g. through the redaction of individuals' residential addresses. We also intend to allow applications for exemptions from public disclosure in certain cases.

We have consulted widely on the policy and this element specifically, and taken those views into account.

We will also seek to take a power in the legislation which will allow us to add or remove data fields should the need arise.

We have considered the European Convention on Human Rights (ECHR) implications of this project in the context of the Small Business, Employment and Enterprise Bill. The Secretary of State for Business, Innovation and Skills has made a statement under section 19(1)(a) of the Human Rights Act 1998 that, in his view, the provisions of the Bill (including this policy) are compatible with the Convention rights.

**8. Will the project require you to contact individuals in ways that they may find intrusive?**

**No.**

UK companies will be required to obtain and hold information on their beneficial owners and provide this to a publicly accessible central registry maintained by Companies House. Information may be collected by the company by way of notice

served on the individual, or other means. The company will not be able to enter information in their register (and therefore, this will not be provided to Companies House) unless it has been provided by the individual or with his or her knowledge. However, an individual will not be required to respond to a notice from the company where the request is frivolous or vexatious.

Individuals will also be required to disclose their beneficial interest in the company to the company (unless the company already has this information).

We do not anticipate that Government will have cause to contact these individuals directly, other than in the case of applications for exemption from public disclosure.

There may be some other limited instances in which Companies House needs to contact an individual. There are also likely to be instances in which law enforcement and tax authorities use the information to contact individuals in the context of criminal investigations.

## Annex B: Identification of Risks

**Table 1: Private Register- Risk Solutions**

Risk	Solutions	Result- Is the risk eliminated, reduced or accepted?	Evaluation
<p>Misuse by overseas countries- Inadequate disclosure controls increase the likelihood of information being shared or used inappropriately</p>	<p>We are carefully considering which UK and overseas authorities should be allowed access to the private register and how. We are giving particular consideration to how overseas authorities can access this information quickly and easily, whilst also ensuring that any information shared is appropriately used and stored. We will seek wider stakeholder views on this issue.</p>	<p>Given that the policy around sharing the information with overseas agencies and the protection regime is still being developed, we have not sought to quantify this risk at this stage. However we will ensure that this information is shared appropriately and in line with the Data Protection Principles. We will update the PIA as appropriate as the policy is developed.</p>	<p>We believe that any risk will be necessary and proportionate. The UK has committed to ensuring that the data is shared, subject to appropriate protection measures, with developing countries to improve their ability to, for example, tackle tax evasion etc.</p>
<p>Overseas countries systems are insufficiently secure (e.g. can be hacked into) leading to inappropriate use or transfers of data</p>	<p>We are carefully considering which UK and overseas authorities should be allowed access to the private register and how. We are giving particular consideration to how overseas authorities can access this information quickly and easily, whilst also ensuring that any information shared is appropriately used and stored. We will seek wider stakeholder views on this issue.</p>	<p>Given that the policy around sharing the information with overseas agencies and the protection regime is still being developed, we have not sought to quantify this risk at this stage. However we will ensure that this information is shared appropriately and in line with the Data Protection Principles. We will update the PIA as appropriate as the policy is developed.</p>	<p>We believe that any risk will be necessary and proportionate. The UK has committed to ensuring that the data is shared, subject to appropriate protection measures, with developing countries to improve their ability to, for example, tackle tax evasion etc.</p>

**Table 2: Public Register- Risk Solutions**

Risk	Solutions	Result- Is the risk eliminated, reduced or accepted?	Evaluation
<p>Public harassment- Publishing new data may lead to harassment of these individuals by members of the public (e.g. marketing, hate mail, lobbying).</p>	<p>The information to be contained on the public register is not significantly different to the current information requirements set out by Companies House for company directors. We intend to allow applications to Companies House to protect beneficial ownership information from public disclosure in specified exceptional circumstances and are carefully considering the criteria and process for these applications.</p>	<p>The risk of public harassment occurring as a result of the publication of this register should be reduced by the fact that we have taken steps to mitigate the risk of this by redacting certain pieces of information and will allow exemptions from public disclosure in certain circumstances. The risk is not completely eliminated because the public will still have access to the beneficial owner's name and service address (unless an exemption applies).</p>	<p>We believe that the risk contained is necessary and proportionate for this policy proposal. We are confident that the amount of information to be contained within the register and the proposed exemptions regime support this.</p>
<p>Identity theft- Personal information collected and published may be used by criminals to create fake identities</p>	<p>To mitigate this risk, we have opted to redact the 'day' of the date of birth on the public register, and ensure that residential addresses and full dates of birth are only accessible by specified authorities.</p>	<p>The risk of identity theft should be reduced by the redaction of the 'day' of the date of birth and residential address on the public register. Whilst the risk is not completely eliminated, we are confident that this approach achieves the right balance between ensuring that beneficial owners can be uniquely identified in the vast majority of cases; whilst also protecting individuals from the risk of identity theft and fraud.</p>	<p>We believe that the risk contained is necessary and proportionate for this policy proposal. We are confident that the redaction of residential addresses and the 'day' of the date of birth mitigate this risk.</p>

<p>Fraud or other serious crime (e.g. kidnapping, asset stripping) - Personal information collected and published may be used to commit crime</p>	<p>To mitigate this risk, we have opted to redact the 'day' of the date of birth on the public register, and ensure that residential addresses and full dates of birth are only accessible by specified authorities. A protection regime will be available to those at serious risk of harm.</p>	<p>The risk of crime should be reduced by the redaction of the 'day' of the date of birth and residential address on the public register. Whilst the risk is not completely eliminated, we are confident that this approach achieves the right balance between ensuring that beneficial owners can be uniquely identified in the vast majority of cases; whilst also protecting individuals from the risk of identity theft and fraud.</p>	<p>We believe that the risk contained is necessary and proportionate for this policy proposal. We are confident that the redaction of residential addresses and the 'day' of the date of birth mitigates this risk.</p>
<p>Collection of information about vulnerable people- Vulnerable people may be particularly concerned about the risks of identification or the disclosure of information.</p>	<p>Vulnerable people in this case means those at risk of serious harm. To mitigate this risk, we intend to allow applications to Companies House to protect beneficial ownership information from public disclosure in specified exceptional circumstances. We are carefully considering the criteria and process for these applications. This will be taken forward through secondary legislation.</p>	<p>The concerns of vulnerable people about the collection and publication of personal information should be significantly reduced by the option to protect beneficial ownership information from public disclosure in specified exception circumstances. However, given that the individual will likely have to apply to Companies House to be exempted from public disclosure, we cannot mitigate the risk for those who choose not to apply but may be vulnerable for one reason or another. Where notice is served by a company on an individual, we intend that the process for applications for exemptions from public disclosure will be included in the notice.</p>	<p>We believe that the procedures in place are sufficient to mitigate the risk to vulnerable people within this proposal.</p>

<p>Intrusiveness- Measures taken against individuals as a result of collecting information about them may be seen as intrusive.</p>	<p>We have carefully considered the impact that this policy has on the privacy of individuals. We anticipate that this proposal will have an impact on the amount of data collected on individuals but are confident that these measures are necessary and proportionate. To aid this, we published our discussion paper in July 2013 and sought views from stakeholders on what information should be included in the central registry of company beneficial ownership information. We have ensured that we have taken these views into account when developing our proposals in relation to this.</p>	<p>We accept that there is a risk that some people who are required to submit their information may see this as an intrusion of their privacy. However, we believe that this risk is reduced by our engagement with stakeholders and the fact that their views have been built into our thinking. The information to be contained on the central registry of beneficial ownership is not significantly different to the current information requirements set out by Companies House for company directors, and some beneficial owners will also be company directors. That should further reduce the likelihood of this collection of data being seen as intrusive.</p>	<p>We are confident that our proposed approach achieves the right balance between ensuring that beneficial owners can be uniquely identified in the vast majority of cases; whilst also protecting individuals from excessive intrusion.</p>
---	---	---	--



## Annex C: Linking the guidance to the Data Protection principles

In addition to the above, we have identified where our policy will fit in with the Data Protection Act Principles. This analysis is outlined below.

### Principle 1

**Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:**

**a) at least one of the conditions in Schedule 2<sup>10</sup> is met, and**

**b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.**

1. Have you identified the purpose of the project?

Yes. Company records (held by the company and at Companies House) provide information about a company's directors and members ("shareholders"). But companies are not currently required to provide information about the individuals who ultimately own and control the company - the 'beneficial owners' or 'people with significant control'.

Companies can be used as a front to facilitate crime, from money laundering and terrorist financing to tax evasion and drug trafficking. Elaborate and opaque ownership structures to obscure the beneficial ownership of a company can play a part in this.

The policy intends to ensure that UK companies obtain and hold adequate, accurate and current information on their beneficial ownership; and make this information publicly accessible onshore in a central registry. The registry should provide a single source of information to support national and overseas law enforcement and tax authorities' investigations; support financial institutions and other regulated professional bodies as they carry out anti-money laundering due diligence checks on companies; and allow all those who engage with a company (e.g. investors, suppliers, customers) to identify with whom they are really doing business. The overarching policy objectives are to reduce crime and improve the business environment so as to facilitate economic growth. The UK has determined that these policy objectives can be best served through greater transparency (i.e. by making information publicly accessible).

The policy is consistent with the implementation of international recommendations made by the Financial Action Task Force (FATF); draft proposals under the Fourth

---

<sup>10</sup> Legislative references in this Annex are to the Data Protection Act 1998 unless otherwise specified.

Money Laundering Directive; and commitments made by the UK in the context of the G8 in 2013.

2. How will you tell individuals about the use of their personal data?

Companies will not be able to enter information in their register (and therefore provide this information to Companies House) unless it has been provided by the individual or with his or her knowledge (whether proactively or in response to a notice issued by the company).

We intend that any notice issued by a company will set out what information is required; what information will be made available publicly by the company and at Companies House and the process by which individuals may apply for an exemption from public disclosure. This will be set out in secondary legislation.

3. Do you need to amend your privacy notices?

No. The current privacy notice on the Companies House website covers our proposal.

4. Have you established which conditions for processing apply?

The processing will be necessary for the exercise of functions conferred on persons under proposed amendments to the Companies Act 2006, contained in the SBEE Bill. See paragraph 5(b) of Schedule 2 to the DPA.

We will not collect any sensitive personal data under this policy. There may be circumstances in which a person may infer certain sensitive information about an individual as a result of their association with a company (for example, where a company is known to have strong links to a certain political party).

We will consider such instances as we develop our protection regime. The regime will suppress data from the public record where an individual might otherwise be at serious risk.

5. If you are relying on consent to process personal data, how will this be collected and what will you do if it is withheld or withdrawn?

We are not relying on consent to process personal data. Information will be collected and processed in line with statutory obligations and requirements.

6. If your organisation is subject to the Human Rights Act, you also need to consider:

Will your actions interfere with the right to privacy under Article 8?

We have considered carefully the effect of this policy in relation to the Article 8 right to privacy, and consider that any interference is justified and proportionate, and necessary for valid reasons in a democratic society. In the context of the Small Business, Employment and Enterprise Bill the Secretary of State for Business, Innovation and Skills has made a statement under section 19(1)(a) of the Human Rights Act 1998 that, in his view, the provisions of the Bill (including this policy) are compatible with the Convention rights.

*In summary:*

We do not believe that our proposal to implement a central registry of company beneficial ownership information contravenes our commitments to the European Convention on Human Rights (ECHR).

Article 8, section one of the ECHR states that:

***“Everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of [...] the prevention of disorder or crime [...]”.***

Implementation of a publicly accessible central registry of company beneficial ownership information means that we are exposing personal data on individuals with a significant beneficial interest in a UK company to anyone who chooses to search for it. However, it is important to note that:

- similar information is already being held on the public record - for example, on company shareholders and directors; and some of the required beneficial ownership information will already be in the public domain (e.g. where the company director is the company’s beneficial owner);
- only information on individuals with a significant beneficial interest in a UK company will be held (i.e. individuals with an interest in more than 25% of the company’s shares or voting rights; or who otherwise control the way the company is run); and
- we intend that there will be a framework of exemptions from public disclosure for individuals at risk.

In addition, one of the policy objectives is to reduce crime through tackling the potential for misuse of companies; and there is international agreement (for example, at G7 and through the FATF standards) around the importance of enhanced corporate transparency. This further justifies our analysis that our proposal does not contravene our ECHR commitments.

#### 7. Have you identified the social need and aims of the project?

Yes. In addition to the purpose of the project outlined above, the policy should also:

- Stimulate global, collective action to tackle the misuse of companies. Investigations into abuses of company structures will often cross borders and so coordinated international action is vital. In leading by example, UK and G7 action should encourage other jurisdictions, including the UK's Overseas Territories and Crown Dependencies, to follow suit. This should deliver better outcomes in terms of reducing crime in the UK as well as elsewhere;
- Deliver benefits for developing countries who suffer as a result of tax evasion, corruption and fraud. By allowing them access to information on UK companies, they should be more easily able to identify the individuals really responsible where a UK corporate entity has been used to facilitate the crime;
- Prevent or deter crime which will have a positive impact on individuals' well-being (as an example, the social and economic costs of organised crime in the UK are estimated to be £24bn<sup>11</sup>, of which £8.9bn are associated with fraud); and
- Ensure full UK compliance with relevant international standards in advance of the UK's next FATF peer review in 2016 to maintain and enhance the UK's reputation as a clean and trusted place to do business and invest.

8. Are your actions a proportionate response to the social need?

Yes.

The reasons for this are outlined in the purpose and social need aspects of the principles.

## Principle 2

**Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.**

9. Does your project plan cover all of the purposes for processing personal data?

Yes.

Processing will be necessary by companies and Companies House for compliance with amendments to the Companies Act 2006.

The public register at Companies House will contain information on the beneficial owners':

- full name;

---

<sup>11</sup> Home Office (October 2013): *Serious and Organised Crime Strategy*. This estimate does not include money laundering.

- month and year of birth<sup>12</sup>;
- nationality;
- country or state of usual residence;
- a service address; and
- date on which they acquired the beneficial interest in the company and the nature of their control over the company.

Companies House will also hold a residential address and a full date of birth for the beneficial owner. This information will however only be accessible to specified authorities.

We are considering which UK and overseas authorities should have access to protected information held at Companies House, and how to ensure that this is as easy and cheap as possible whilst also ensuring that data is appropriately stored and held.

10. Have you identified potential new purposes as the scope of the project expands?

No.

### Principle 3

**Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.**

11. Is the quality of the information good enough for the purposes it is used?

The intention is that the required particulars will allow those looking at the register to **uniquely** identify the individual recorded as the beneficial owner in the vast majority of cases; and to build a meaningful picture of the company's overarching ownership and control structure – both as at the date the register is inspected and previously.

The data to be obtained and held is necessary to meet the primary objectives of the policy, as set out in this document.

The public register at Companies House will therefore contain information on the beneficial owners':

- full name;
- month and year of birth<sup>13</sup>;
- nationality;
- country or state of usual residence;
- a service address;

---

<sup>12</sup> Unless the company has opted to maintain its register at Companies House.

<sup>13</sup> Unless the company has opted to maintain its register at Companies House.

- date on which they acquired the beneficial interest in the company and the nature of their control over the company.

Companies House will also hold a residential address and a full date of birth for the beneficial owner. This information will however only be accessible to specified authorities.

The information to be held and made available publicly is consistent with the information held on company directors, with the exception of information that is relevant for directors but not beneficial owners (i.e. former business name and business occupation).

12. Which personal data could you not use, without compromising the needs of the project?

None. We are confident that our proposed approach achieves the right balance between ensuring that beneficial owners can be uniquely identified in the vast majority of cases; whilst also protecting individuals from the risk of identity theft and fraud.

We will however seek to take a power in the primary legislation to add to or remove from the data fields should the need arise (e.g. should we identify that more, less or different data would better meet the policy objectives).

#### **Principle 4**

**Personal data shall be accurate and, where necessary, kept up to date.**

13. If you are procuring new software does it allow you to amend data when necessary?

N/A

14. How are you ensuring that personal data obtained from individuals or other organisations is accurate?

Companies will not be able to enter information in their register (and therefore provide this information to Companies House) unless it has been provided by the individual or with his or her knowledge (whether proactively or in response to a notice issued by the company).

This should ensure that data is accurate, supported by the fact that the register is publicly accessible (so can be scrutinised for inaccuracies) and that the false provision of information will be a criminal offence.

In addition, we will require companies to update the information held in their register of beneficial owners if they knew or might reasonably be expected to have known

that a change to their beneficial ownership had occurred. We will also require beneficial owners to inform the company of any changes to the information recorded in the register of beneficial owners.

We will require companies to provide an initial statement of beneficial ownership on incorporation. We will also require companies to update their beneficial ownership information at least once in a 12 month period. We intend to take this forward in the context of the new 'check and confirm' system (which will make changes to the existing annual return process), requiring all changes to beneficial ownership that have occurred in-year to be listed.

We want all companies to be as transparent as possible and keep their information as up to date as possible. That is why companies will be able to update the information held at Companies House more frequently should they wish to do so. In addition, private companies will have the option to maintain and update their beneficial ownership register at Companies House directly – meaning that changes would be updated at Companies House as the company becomes aware of them.

Companies House recognises that register integrity is an important issue, and is currently carefully considering whether any further reform is necessary in terms of verifying or checking information on the register - whilst ensuring the UK's company registration regime remains quick, simple and inexpensive.

## **Principle 5**

**Personal data processed for any purpose or purposes shall not be kept for longer than necessary for that purpose or those purposes.**

### 15. What retention periods are suitable for the personal data you will be processing?

Data will remain on the company's register for 10 years after the date on which a person ceases to be a beneficial owner. This is consistent with the retention period that applies in respect of company shareholders and we are satisfied that it is appropriate in the context of this reform.

Information is delivered to the registrar under statute. Companies House is therefore exempt under section 34 of the DPA from the majority of the Data Protection Principles. The Companies Act 2006 requires the registrar to make the information available for public inspection including the right to a copy (see section 1085 and section 1086) except in certain cases (see for example section 240 and section 1087).

Data will remain on the register at Companies House indefinitely unless the company is dissolved. In that case the registrar may direct the records to the Public Record Office a minimum of two years after the dissolution. Beyond this there is no need to consider retention because of the general exemption from the 5th Principle of the DPA.

16. Are you procuring software that will allow you to delete information in line with your retention periods?

N/A

Companies will provide the information to Companies House under statute. Section 34 of the DPA exempts the registrar from the 5th Principle of the DPA. Section 1084 of the Companies Act 2006 otherwise provides for how records of dissolved companies may be disposed.

## **Principle 6**

**Personal data shall be processed in accordance with the rights of data subjects under this Act.**

17. Will the systems you are putting in place allow you to respond to subject access requests more easily?

N/A

The data on the public register will be accessible by the subject from Companies House in the same way as any other information held by Companies House, for example on directors and shareholders. Data withheld from public inspection will only be accessible by specified bodies under specified conditions. Section 34 of the DPA also exempts the registrar from the requirement to comply with subject access requests.

18. If the project involves marketing, have you got a procedure for individuals to opt out of their information being used for that purpose?

N/A

## **Principle 7**

**Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.**

19. Do any new systems provide protection against the security risks you have identified?

No. Existing systems will be used, as they are for directors' information.



20. What training and instructions are necessary to ensure that staff know how to operate a new system securely?

Existing systems will be used, as they are for directors' information.

### **Principle 8**

**Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures and adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.**

21. Will the project require you to transfer data outside of the EEA?

The transfer of data should be divided into the information on the public register and the information on the private register.

#### Public Register

The 8th Principle of the DPA provides that data must not be transferred outside the European Economic Area (EEA) unless adequate levels of protection are in place in relation to the processing of personal data.

However, data on the public register is exempt from the 8th Principle by virtue of Schedule 4 to the DPA.

In terms of data transfer, information on the public register will therefore be held, used and disclosed in line with the provisions of the Companies Act 2006 and the DPA, where applicable.

#### Private Register

We use 'private register' to refer to information held by Companies House which is not made available publicly, namely residential addresses, full dates of birth and information on individuals whose information is to be withheld from public inspection. We are carefully considering which UK and overseas authorities should be allowed access to the private register and how. We are giving particular consideration to how overseas authorities can access this information quickly and easily, whilst also ensuring that any information shared is appropriately used and stored.

This element of the policy will be set out in secondary legislation and we intend to seek wider stakeholder views on this. Proposed options will take full account of the Data Protection Principles and we will update the PIA as necessary.

22. If you will be making transfers, how will you ensure that the data is adequately protected?

We are carefully considering which UK and overseas authorities should be allowed access to the private register and how. Policy options will be developed as we further refine and develop the policy, taking full account of the Data Protection Principles.

# Bearer Shares: Privacy Impact Assessment

## What is a privacy impact assessment?

1. A privacy impact assessment is a process which helps an organisation to identify and reduce the privacy risks of a project. An organisation should use a PIA throughout the development and implementation of a project, and can use existing project management processes. A PIA enables an organisation to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.
2. The purpose of the PIA is to minimise privacy risks while meeting the aims of the project. Organisations can identify and address risks at an early stage by analysing how the proposed uses of personal information and technology will work in practice. They can test this analysis by consulting with people who will be working on, or affected by, the project.
3. Conducting a PIA is not a legal requirement of the DPA. The ICO promotes PIAs as a tool which will help organisations to comply with their DPA obligations, as well as bringing further benefits. Carrying out an effective PIA should benefit the people affected by a project and also the organisation carrying out the project.
4. More information on PIAs can be found in the ICO's guidance document.

## What do we mean by privacy?

5. Privacy, in its broadest sense, is about the right of an individual to be let alone. It can take two main forms, and these can be subject to different types of intrusion:
  - Physical privacy - the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.
  - Informational privacy – the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online. It extends to monitoring the records of senders and recipients as well as the content of messages.

## Objective

6. The objective of conducting this PIA is to identify any data protection issues in relation to the company directors' transparency and accountability section of the Transparency and Trust package. The PIA will identify any potential privacy risks and focus on whether the policy complies with the Data Protection Act and other relevant legislation.

## PIA Process

7. The screening process for this PIA was conducted in accordance with the ICO guidance in August 2010, as this was the most current document when the screening processes were commissioned. This guidance is attached.
8. The PIA process is a flexible one, and an organisation can integrate it with their existing approach to managing projects. The ICO's handbook suggests undergoing a screening process to determine the key data protection and security issues of a particular proposal. The responses to these questions will indicate whether a full scale PIA is required, or if a small scale assessment is sufficient. The process for undertaking both assessments is the same, but the level of detail is different. To perform a PIA adequately, Government officials are advised to work their way through both sets of questions.

## Step 1 – Criteria for full scale PIA

9. The first part of the screening process is a series of 11 questions focusing on issues including technology, identity, multiple organisations, data, exemptions and exceptions. The answers to the questions need to be considered as a whole to decide whether the overall impact and the related risk warrant a full scale PIA.

## Step 2 – Criteria for small scale PIA

10. These questions should be considered to determine whether a small scale PIA is required.
11. If the results of both sets of screening questions suggest that a PIA is not required, then a check will still be required to ensure that the policy or project meets the requirements of the DPA. These Data Protection Principles are outlined below:

## Data Protection Principles

12. The DPA regulates the processing of personal data through an enforceable set of good practice handling rules known as the data protection principles.

13. The eight data protection principles are expressed in general terms, and state that personal data must be:
- Fairly and lawfully processed;
  - Processed for specific and lawful purposes and not further processed in a way that is incompatible with the original purpose;
  - Adequate, relevant and not excessive;
  - Accurate and up to date;
  - Not kept for longer than is necessary;
  - Processed in accordance with the data subject's rights;
  - Kept secure;
  - Not transferred to countries outside the European Economic Area unless an adequate level of protection is ensured or an exemption applies.

## Objectives of the policy

1. At the G8 Summit in 2013, G8 Leaders recognised the problem of corporate opacity and agreed to publish national Action Plans setting out the concrete steps they would take to address this. The UK's Action Plan set out a number of commitments, including commitments in relation to the use of bearer shares. These commitments reinforced other international standards. The commitments have since been developed as part of BIS' *Transparency and Trust* package.
2. Corporate opacity can facilitate illicit activity, and can lead to poor corporate oversight which erodes trust and damages the business environment. Both crime and a lack of trust can impede economic growth.
3. Although bearer shares can be used for legitimate purposes, the Global Forum on Transparency and Exchange of Information for Tax Purposes (Global Forum) and Financial Action Task Force (FATF) have both identified bearer shares as high risk and as useful for criminals, facilitating tax evasion and money laundering. A number of jurisdictions have now banned them, and it is important for the reputation of the UK that we act to meet international standards and commitments.
4. Bearer shares certify the bearer of the warrant is entitled to the shares represented by it. This means the legal ownership of the share can be transferred simply by passing the physical share warrant from one person to another - there is no record of ownership, or change of ownership, on the company's register of members. These shares are therefore a means for individuals to avoid any record of their ownership of a stake in a company, so allowing them to conceal or transfer control. There is an inherent lack of transparency.

## What does the policy set out to achieve?

5. The overarching policy objectives of the *Transparency and Trust* package are to reduce crime and improve the business environment so as to facilitate economic growth. Specifically, the objective of this policy is to ensure that the UK fully meets Global Forum and FATF standards with respect to bearer shares and remove the opacity they introduce.
6. To do this, the policy approach is to:
  - Prohibit the creation of new bearer shares
  - Provide a nine month period for the conversion of existing bearer shares to registered shares. The nine month period balances the need for swift action with a reasonable period for adjustment.
  - Require companies, after the nine month period, to apply to court to cancel any remaining shares.
7. As part of the process of reform, information about the detail of the change and how to comply will be disseminated through Government channels.

## Who is affected by the policy?

8. Analysis indicates that just over 1200 UK companies have issued bearer shares. From a total population of 3.19 million companies, this figure represents 0.04% of companies. The use of bearer shares is not therefore widespread – but it is problematic.
9. By the very nature of bearer shares we cannot know how many shareholders own these, but we estimate there might be around 3000<sup>14</sup> bearer shareholders of UK companies.

## Impact

10. We have completed the required screening process for this policy and are satisfied that a PIA does not need to be completed. The screening assessment at Annexes A and B covers the policy of bearer shares to be contained in primary legislation.
11. Where the screening process has identified areas involving identity we have shown the need for the policy change.

---

<sup>14</sup> For further discussion please see the related Impact Assessment which covers the costs and benefits of the policy change.

12. It is the very anonymous nature of bearer shares that requires us to take action. The policy behind the abolition of share warrants is in the public interest to prevent crime by reducing the opportunities for money laundering and ensure taxes are paid. The public interest for this action is shown in the internationally agreed necessity to take specific measures to prevent the misuse of mechanisms that are frequently used to disguise the ownership of companies. The proposal is essentially amending the form that the bearer shareholder's rights take, rather than the rights themselves. The related data requirements would become aligned with those required for other types of shares in the UK.
13. We are confident that the policy meets the data protection principles outlined above.

## Annex A: Screening process for a small scale PIA

### Technology:

*Does the proposal involve new technologies or technologies that can substantially reveal personal information, such as visual surveillance, digital image and video recording?*

**No.**

### Justification:

*Is the justification for the new data-handling unclear or unpublished?*

**No.**

We have published our proposals for views<sup>15</sup>, and then in a document responding to those views<sup>16</sup>. In April 2014 we confirmed our intention to abolish bearer shares, prohibiting their issue and requiring the conversion of existing bearer shares. Ongoing stakeholder engagement (for instance to develop the detail of the conversion process) has confirmed widespread support for the overall principle of abolition. There has been some discussion of privacy, but it has not been a central issue in our interactions with a wide range of interested and expert parties over a number of months.

### Identity:

*Does the proposal involve an additional use of an existing identifier?*

**No.**

Where current bearer share holders respond to the policy change by holding their shares as registered shares, they will need to be entered into the company's register of members like all other shareholders. New shareholders who would otherwise have used bearer shares but are no longer able to do so (when they become unlawful) will also need to use registered share arrangements. Depending on the alternative approach chosen, some identifiers will be entered into the company's register and provided to Companies House. Use of existing identifiers that currently apply to all shareholders will therefore be extended to cover this small group.

---

<sup>15</sup> *Transparency and Trust* discussion paper (July 2013)  
([https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/212079/bis-13-959-transparency-and-trust-enhancing-the-transparency-of-uk-company-ownership-and-increasing-trust-in-uk-business.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/212079/bis-13-959-transparency-and-trust-enhancing-the-transparency-of-uk-company-ownership-and-increasing-trust-in-uk-business.pdf))

<sup>16</sup> *Transparency and Trust* government response to views received (April 2014)  
([https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/304297/bis-14-672-transparency-and-trust-consultation-response.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/304297/bis-14-672-transparency-and-trust-consultation-response.pdf))



*Does the proposal involve use of a new identifier for multiple purposes?*

**No.**

*Does the proposal involve new or substantially changed identity authentication requirements that may seek excessive personal information or be onerous upon an individual? It is important that identity authentication is proportionate to the purpose. For example, in some situations face to face contact may have a lower threshold for identity authentication while electronic transactions may have a higher threshold of authentication and may seek more than one assurance.*

**No.**

**Data:**

*Will the proposal result in the handling of a significant amount of new personal data about each person, or significant change in existing data-holdings?*

**No.**

Where current bearer share holders respond to the policy change by holding their shares as registered shares, they will need to be entered into the company's register of members like all other shareholders. New shareholders who would otherwise have used bearer shares but are no longer able to do so (when they become unlawful) will also need to use registered share arrangements. Depending on the alternative approach chosen, some identifiers will be entered into the company's register and provided to Companies House<sup>17</sup>. Use of existing identifiers that currently apply to all shareholders will therefore be extended to cover this small group.

*Will the proposal result in the handling of new personal data about a significant number of people or a significant change in the population coverage?*

**No.**

*Does the proposal involve new linkage of personal data with data in other collections, or significant change in data linkages?*

**No.**

Where current bearer share holders respond to the policy change such that basic personal data is provided to Companies House, this data will be available alongside but not linked to other data available at Companies House.

---

<sup>17</sup> Please see separate Privacy Impact Assessment covering Company Filing Requirements. This covers further reforms to allow private companies to opt out of keeping out of the requirement to keep the company registers and, instead, keep the information on the public register, and considered the implications thereof.

**Data handling:**

*Does the proposal involve new or different data collection policies or practices that may be unclear or seek excessive information that is not relevant to the purpose? Data controllers should seek to identify the minimum amount of information that is required in order properly to fulfil their purpose. Processing excessive amounts of information that is not required for the purposes of the data controller will be in breach of the data protection principles.*

**No.**

The data requirements for current bearer share holders who respond to the policy change by holding their shares transparently will be the same as for other shareholders; therefore we have no reason to believe they would be excessive. As set out above the information requirements for shareholders are not excessive.

As part of the nine month conversion period for existing bearer shares, some new pieces of information will be required by the court or the Registrar of companies. These pieces of information relate to the company, rather than to identifiers.

*Does the proposal involve new or different data quality assurance processes and standards that may be unclear or unsatisfactory?*

**No.**

*Does the proposal involve new or different data security arrangements that may be unclear or unsatisfactory?*

**No.**

*Does the proposal involve new or different data access or disclosure arrangements that may be unclear or permissive?*

**No.**

*Does the proposal involve new or different data retention arrangements that may be unclear or extensive?*

**No.**

*Does the proposal involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?*

**No.**

Where the policy change results in increased use of registered shares, some identifiers will be entered into the company's register and provided to Companies House. However the medium of disclosure at Companies House will be the same as currently applies for all other shareholders; it will not change.

**Exceptions:**

*Will the proposal give rise to new or changed data-handling that is in any way exempt from legislative data protection measures? This could include, for example, national security information systems.*

**No.**

## Annex B: Screening process for a full scale PIA

### Technology:

*Does the proposal apply new or additional information technologies that could affect an individual such as locator technologies (including mobile phone location)?*

**No.**

### Identity:

*Does the proposal involve new identifiers or re-use of existing identifiers, such as digital signatures?*

**No.**

Government policy on the identifiers required for shareholders will not change as part of the reforms to abolish bearer shares. Bearer share holders will become registered shareholders and meet the data requirements associated with being a registered shareholder. Information is held in a company's register of members and / or provided to Companies House (on the public record).

- name of shareholder (or changes to name)
- number of shares of each class held
- date of registration
- number of shares of each class transferred since previous annual return (or since incorporation if this is the first)

Traded public companies, or companies whose shares are traded on a relevant market, must provide:

- full list of shareholders names and addresses who hold 5% or more of share capital
- number of shares of each class held
- date of registration
- number of shares of each class transferred since previous annual return (or since incorporation if this is the first)

Changes to the wider process for providing such information to Companies House are covered in a separate PIA. Where a bearer share holder is also a person of significant control this might affect information required of them in that capacity; the impact of the register of people of significant control is also considered in a separate PIA.

*Might the proposal have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?*

**Yes (can no longer hold anonymously or transfer anonymously).**

The abolition of bearer shares will essentially amend the form that the bearer share holder's rights take, rather than the rights themselves. The related data requirements would become aligned with those required for other types of shares in the UK.

The abolition of bearer shares would result in the removal of a shareholding instrument that permits the shareholder to remain anonymous. This means it would no longer be possible for them to conceal or anonymously transfer their ownership of a stake in a company. In this instance it is the very anonymous nature of the shares that requires us to take action.

The abolition of share warrants is in the public interest to prevent crime by reducing the opportunities for money laundering and ensure taxes are paid. The public interest is shown in the internationally agreed necessity to take specific measures to prevent the misuse of mechanisms that are frequently used to disguise the ownership of companies.

There are routes to protecting identity with respect to shareholdings, which are currently available and will remain accessible and acceptable. A significant difference is the presence of a paper trail and formal process, meaning law enforcement can pursue issues where criminal activity is suspected.

**Multiple Organisations:**

*Does the proposal involve multiple organisations, whether they are Government agencies (for example in "joined-up Government" initiatives) or private sector organisations (for example, as outsourced service providers or as "business partners")?*

**No.**

**Data:**

*Does the proposal involve new or significantly different handling of personal data that may be of particular concern to individuals?*

**No.**

Where current bearer share holders respond to the policy change by holding their shares as registered shares, they will need to be entered into the company's register of members like all other shareholders. New shareholders who would otherwise have used bearer shares but are no longer able to do so (when they become unlawful) will also need to use registered share arrangements. Depending on the alternative approach chosen, some identifiers will be entered into the company's register and

provided to Companies House<sup>18</sup>. There will be no change to the handling of data relative to the mechanisms that currently apply to shareholders.

*Does the proposal involve new or significantly different handling of a considerable amount of personal data about each individual in the database?*

**No.**

*Does the proposal involve new or significantly different handling of personal data about a large number of individuals?*

**No.**

*Does the proposal involve new or significantly different consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?*

**No.**

**Exemptions:**

*Does the proposal relate to data processing which is in any way exempt from legislative data protection measures, for example, processing of personal data for the purposes of national security?*

**No.**

*Does the proposal's justification include significant contributions to public security measures, for example, serious convicted offenders who have served their sentence and are released into the community. In these cases, personal data may need to be shared to ensure the safety of the public.*

**No.**

*Does the proposal involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable data protection regulation?*

**No.**

---

<sup>18</sup> Please see separate Privacy Impact Assessment covering Company Filing Requirements. This covers further reforms to allow private companies to opt out of keeping out of the requirement to keep the company registers and, instead, keep the information on the public register, and considered the implications thereof.

# Company Directors: Privacy Impact Assessment

## What is a privacy impact assessment?

1. A privacy impact assessment is a process which helps an organisation to identify and reduce the privacy risks of a project. An organisation should use a PIA throughout the development and implementation of a project, and can use existing project management processes. A PIA enables an organisation to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.
2. The purpose of the PIA is to minimise privacy risks while meeting the aims of the project. Organisations can identify and address risks at an early stage by analysing how the proposed uses of personal information and technology will work in practice. They can test this analysis by consulting with people who will be working on, or affected by, the project.
3. Conducting a PIA is not a legal requirement of the DPA. The ICO promotes PIAs as a tool which will help organisations to comply with their DPA obligations, as well as bringing further benefits. Carrying out an effective PIA should benefit the people affected by a project and also the organisation carrying out the project.
4. More information on PIAs can be found in the ICO's guidance document.

## What do we mean by privacy?

5. Privacy, in its broadest sense, is about the right of an individual to be let alone. It can take two main forms, and these can be subject to different types of intrusion:
  - Physical privacy - the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.
  - Informational privacy – the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online. It extends to monitoring the records of senders and recipients as well as the content of messages.

## Objective

6. The objective of conducting this PIA is to identify any data protection issues in relation to the company directors' transparency and accountability section of the Transparency and Trust package. The PIA will identify any potential privacy risks and focus on whether the policy complies with the Data Protection Act and other relevant legislation.

## PIA Process

7. The screening process for this PIA was conducted in accordance with the ICO guidance in August 2010, as this was the most current document when the screening processes were commissioned. This guidance is attached.
8. The PIA process is a flexible one, and an organisation can integrate it with their existing approach to managing projects. The ICO's handbook suggests undergoing a screening process to determine the key data protection and security issues of a particular proposal. The responses to these questions will indicate whether a full scale PIA is required, or if a small scale assessment is sufficient. The process for undertaking both assessments is the same, but the level of detail is different. To perform a PIA adequately, Government officials are advised to work their way through both sets of questions.

## Step 1 – Criteria for full scale PIA

9. The first part of the screening process is a series of 11 questions focusing on issues including technology, identity, multiple organisations, data, exemptions and exceptions. The answers to the questions need to be considered as a whole to decide whether the overall impact and the related risk warrant a full scale PIA.

## Step 2 – Criteria for small scale PIA

10. These questions should be considered to determine whether a small scale PIA is required.
11. If the results of both sets of screening questions suggest that a PIA is not required, then a check will still be required to ensure that the policy or project meets the requirements of the DPA. These Data Protection Principles are outlined below:

## Data Protection Principles

12. The DPA regulates the processing of personal data through an enforceable set of good practice handling rules known as the data protection principles.



13. The eight data protection principles are expressed in general terms, and state that personal data must be:

- Fairly and lawfully processed;
- Processed for specific and lawful purposes and not further processed in a way that is incompatible with the original purpose;
- Adequate, relevant and not excessive;
- Accurate and up to date;
- Not kept for longer than is necessary;
- Processed in accordance with the data subject's rights;
- Kept secure;
- Not transferred to countries outside the European Economic Area unless an adequate level of protection is ensured or an exemption applies.

## Objectives of the policy

14. At the G8 Summit in 2013, the G8 Leaders recognised the problem of corporate opacity and agreed to publish national Action Plans setting out the concrete steps they would take to address this. The UK's Action Plan set out a number of commitments, including commitments in relation to opacity around company directors. These have since been developed as part of BIS' *Transparency and Trust* package.

15. Corporate opacity can facilitate illicit activity, and can lead to poor corporate oversight which erodes trust and damages the business environment. Both crime and a lack of trust can impede economic growth.

16. Corporate opacity can arise as a result of opaque arrangements involving company directors. This includes the use of corporate directors, external control of single directors or external control of a board of directors.

17. The use of corporate directors, where one company (or other legal person) acts as the director of another, creates corporate opacity with respect to the individual (or natural person) controlling a company. It could also lead to reduced effectiveness of corporate oversight.

18. In total, there are around 67,000<sup>19</sup> companies with corporate directors in the UK. Notably, despite being limited to 2.1% of all companies, corporate directors feature in cases of financial crime.

19. The use of irresponsible 'front' directors who allow themselves to be controlled by another can similarly introduce opacity of control, and lead to reduced effectiveness of corporate oversight.

---

<sup>19</sup> This figure includes corporate members of LLPs.

20. Since all appointed directors have the same status under the law, there is no means of identifying how many appointed directors are acting irresponsibly as a 'front,' nor how many people are seeking to control them. But we do know that international organisations and UK law enforcement consider such arrangements high risk in terms of facilitating crime such as money laundering.
21. As an indication of what the current system does allow, it is worth noting that 1,223 directors currently act as the director of more than 50 companies, while 6,150 directors currently act as the directors of more than 20 companies. Of course, multiple directorships need not reflect illicit activity or external control of the director (and conversely illicit activity or opaque control can be the product of the use of just one 'front' director in one company)<sup>20</sup>.
22. Moreover, shadow directors will sometimes control all or the majority of a company's directors. In doing so, they have some duties, but these duties are not currently the same as those that apply to a single director (who might have less influence).
23. The goal of the policy is therefore to tackle the scope for abuse and mistrust in the current legal framework which provides for the appointment of corporate directors and a potential lack of accountability for those who control directors.

## What does the policy set out to achieve?

24. The overarching policy objectives of the *Transparency and Trust* package are to reduce crime and improve the business environment so as to facilitate economic growth.
25. To do this, the policy approach is to
- Prohibit the use of corporate directors, with exceptions (potentially applying to companies subject to wider transparency requirements or regulation).
  - Increase the accountability of those who control company directors (while themselves remaining 'off the record') by :
    - Informing directors on appointment of their current statutory duties;
    - Making it possible to disqualify a person who controls a company director and causes misconduct for which they are disqualifiable<sup>21</sup>;
    - Updating the duties that apply to shadow directors who control all or the majority of a company's directors.

---

<sup>20</sup> For further discussion, please see the related Impact Assessment which covers the costs and benefits of the policy change.

<sup>21</sup> Please see the Director Disqualification Privacy Impact Assessment which covers broader measures to update the director disqualification regime.

## Who is affected by the policy?

26. The policy will apply to all companies in the UK, with respect to their directors, and to any persons who control those directors. There should be no differential impact on such persons, based on the protected groups, as a result of this policy – the requirements will apply in the same way to all.
27. In practice, only a small subset of companies will change their behaviour as a result of this policy. That will include:
- i) companies that currently have a corporate director and need to remove it to comply with the prohibition (ie companies that currently have a corporate director who are also out of scope of the exceptions from the prohibition).
  - ii) companies with a registered director or directors controlled by another person, (perhaps as a choice to avoid the increased accountability of the person controlling by a director).
28. We have considered that individuals involved in or with companies who might experience some change would be:
- Putative company directors who are appointed as company directors as a result of the choices companies make in response to the reforms (eg if a corporate director is removed from a company's board and replaced with a natural person)
  - Individual employees of companies that act as corporate directors who need to change their own role in order to maintain a relationship with the directed company
  - Company directors who might consider their role and statutory duties more carefully, or reconsider how far they allow themselves to be controlled by another person in exercising their functions
  - Company directors who might experience change when other directors on their board change (eg when a corporate director alongside them is removed or replaced with a natural person, or when a controlled director chooses to resign) or change their behaviour (eg when a director alongside them is no longer controlled by another person and operates differently)
  - Individual employees of companies who need to handle and register any changes to a company director
  - Anyone outside a company who controls a company director or offers them other advice, and might consider their relationship with the director or directors
29. A wider population might derive benefits from the policy as a result of reduced crime or an improved business environment.
30. We do not consider here a potential deterrent effect or consequences for those who might be using opaque arrangements involving company directors in order to facilitate illicit activity.

## Impact

31. We have completed the required screening process for this policy and are satisfied that a PIA does not need to be completed. The screening assessment at Annexes A and B covers the company directors policy to be contained in primary legislation.
32. Where the screening process has identified risks around data, this risk can be shown to have been mitigated. Where those involved with a corporate director do not wish to become a natural person director under the new system, there is no obligation to do so (and therefore no obligation to provide information to Companies House). Any data provided under the new policy would be the same as data provided under the current system eg provision of details of directors to Companies House. We are confident that the policy meets the data protection principles outlined above.

## Annex A: Screening process for a small scale PIA

### Technology:

*Does the proposal involve new technologies or technologies that can substantially reveal personal information, such as visual surveillance, digital image and video recording?*

**No.**

### Justification:

*Is the justification for the new data-handling unclear or unpublished?*

**No.**

We have published our proposals for views<sup>22</sup>, and then in a document responding to those views<sup>23</sup>. This included restricting the use of corporate directors in the UK, and increasing the accountability of those who control company directors. The proposals have generally been supported. Privacy has not featured as an issue in discussion of the proposals with a wide range of stakeholders over a number of months.

### Identity:

*Does the proposal involve an additional use of an existing identifier?*

**No.**

Government policy on the identifiers required for natural person directors will not change as part of the policy changes described here. Where a new individual natural person director is appointed as a result of the policy change to remove a corporate director, then the current identifiers would apply to them too. This would be as a result of choices made by companies and individuals in response to the policy change, not a requirement of it.

*Does the proposal involve use of a new identifier for multiple purposes?*

**No.**

*Does the proposal involve new or substantially changed identity authentication requirements that may seek excessive personal information or be onerous upon an*

---

<sup>22</sup> *Transparency and Trust* discussion paper (July 2013)

([https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/212079/bis-13-959-transparency-and-trust-enhancing-the-transparency-of-uk-company-ownership-and-increasing-trust-in-uk-business.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/212079/bis-13-959-transparency-and-trust-enhancing-the-transparency-of-uk-company-ownership-and-increasing-trust-in-uk-business.pdf))

*individual? It is important that identity authentication is proportionate to the purpose. For example, in some situations face to face contact may have a lower threshold for identity authentication while electronic transactions may have a higher threshold of authentication and may seek more than one assurance.*

**No.**

**Data:**

*Will the proposal result in the handling of a significant amount of new personal data about each person, or significant change in existing data-holdings?*

**No.**

*Will the proposal result in the handling of new personal data about a significant number of people or a significant change in the population coverage?*

**No.**

Where a new natural person director is appointed as a result of the policy change to remove corporate directors, personal data in relation to those individuals will need to be made available. The data required will be the same as that required of other natural person directors, and include some of the same protections (eg directors' residential addresses are not made public, but held by Companies House only<sup>24</sup>.)

The appointment of a new natural person as a director will be as a result of choices made by companies and individuals in response to the policy change, not a requirement of it.

Where a person is disqualified as a director, limited data is added to a register of disqualified directors. This is to allow business and the public to be aware of directors' misconduct and make informed decisions. Through the present proposal, a person controlling a director can also be disqualified. Their name will therefore be added to the register, as a director's would be. Around 1200 directors are disqualified per annum; it is not expected that the new ground for disqualification of a person controlling a director will result in data relating to a significant number of people being covered by this register.

Wider measures to update the director disqualification regime are considered in a separate PIA.

---

<sup>23</sup> *Transparency and Trust* government response to views received (April 2014) ([https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/304297/bis-14-672-transparency-and-trust-consultation-response.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/304297/bis-14-672-transparency-and-trust-consultation-response.pdf))

<sup>24</sup> Please see the Company Filing Requirements Privacy Impact Assessment which covers changes being made to filing requirements for directors' date of birth.

*Does the proposal involve new linkage of personal data with data in other collections, or significant change in data linkages?*

**No.**

Information relating to company directors is available publicly from Companies House alongside other types of information, but the information will not be linked in new ways as part of this policy change.

**Data handling:**

*Does the proposal involve new or different data collection policies or practices that may be unclear or seek excessive information that is not relevant to the purpose? Data controllers should seek to identify the minimum amount of information that is required in order properly to fulfil their purpose. Processing excessive amounts of information that is not required for the purposes of the data controller will be in breach of the data protection principles.*

**No.**

Data collection policies and practices will not change as part of this policy change. Where a new individual natural person director is appointed as a result of the policy change to remove a corporate director, then the current policies and practices would apply to them too. Since the requirements are the same as for all other directors and are already complied with by 5.7 million directors, we have no reason to believe they are excessive. The data required of directors by law are set out below.

*Does the proposal involve new or different data quality assurance processes and standards that may be unclear or unsatisfactory?*

**No.**

*Does the proposal involve new or different data security arrangements that may be unclear or unsatisfactory?*

**No.**

*Does the proposal involve new or different data access or disclosure arrangements that may be unclear or permissive?*

**No.**

*Does the proposal involve new or different data retention arrangements that may be unclear or extensive?*

**No.**

*Does the proposal involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?*

**No.**

Where a new individual natural person director is appointed as a result of the policy change to remove a corporate director, then information will be disclosed publicly on a new group of people. However, the medium of disclosure will not change as part of this policy change.

**Exceptions:**

*Will the proposal give rise to new or changed data-handling that is in any way exempt from legislative data protection measures? This could include, for example, national security information systems.*

**No.**



## Annex B: Screening process for a full scale PIA

### Technology:

*Does the proposal apply new or additional information technologies that could affect an individual such as locator technologies (including mobile phone location)?*

**No.**

### Identity:

*Does the proposal involve new identifiers or re-use of existing identifiers, such as digital signatures?*

**No.**

Government policy on the identifiers required for individual natural person directors will not change as part of this policy change. Where a new individual natural person director is appointed as a result of the policy change to remove a corporate director, then the current identifiers would apply to them too.

The identifiers currently required to be provided to Companies House for an individual director are set out in the Companies Act 2006 and include

- a) any name and former name
- b) a service address
- c) country of residence
- d) nationality
- e) occupation
- f) date of birth<sup>25</sup>
- g) residential address – not on the public record at Companies House

New information will be required from companies who appoint corporate directors where they are permitted to do so (where they are in scope of exceptions from the wider prohibition). This will not relate to individuals.

*Might the proposal have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?*

Currently, the appointment of a corporate director might allow some individuals to act as company directors without disclosing their details in the same way that all other company directors are required to.

---

<sup>25</sup> Please see the Company Filing Requirements Privacy Impact Assessment which covers changes being made to filing requirements for directors' date of birth.

The policy change will reduce anonymity of control of companies where it is achieved by use of corporate directors. This will reduce the potential for crime and increase transparency in the business environment, both of which will help support economic growth.

The policy change will also deter anonymous control of individual company directors by increasing accountability for the people who stand behind directors. No new data requirements are involved.

It is a longstanding tenet of European and UK company law that the directors of a company are required to make certain pieces of information available. This transparency helps customers, trading partners and investors etc, as well as law enforcers, to know who is engaged in the management of a company. It facilitates effective transactions. In the UK currently there are 5.7 million company directors (in relation to whom information is made available at Companies House) and 67,000<sup>26</sup> corporate directors.

Where those involved with a corporate director do not wish to become a natural person director under the new system, there is no obligation to do so (and therefore no obligation to provide information to Companies House). It is worth noting that anonymity is not the main attraction of corporate directorships among legitimate companies we have surveyed.

Where individuals controlling a director choose, given the increased accountability, to go on the record as a director themselves, there is no obligation to do so.

### **Multiple Organisations:**

*Does the proposal involve multiple organisations, whether they are Government agencies (for example in “joined-up Government” initiatives) or private sector organisations (for example, as outsourced service providers or as “business partners”)?*

**No.**

### **Data:**

*Does the proposal involve new or significantly different handling of personal data that may be of particular concern to individuals?*

**No.**

---

<sup>26</sup> This figure includes corporate members of LLPs.

Where new individual natural person directors are registered in response to the policy change to restrict the use of corporate directors, current data requirements will reply to this new, small, and self-selecting group of individuals.

We do not anticipate that the data required of directors is concerning to them, since 5.7 million directors in the UK provide it currently, and this was not mentioned in the consultation we have undertaken on this proposal (nor indeed the proposal to alter the information available publicly at Companies House covering a directors' date of birth, elsewhere in this package and covered in a separate PIA).

*Does the proposal involve new or significantly different handling of a considerable amount of personal data about each individual in the database?*

**No.**

The amount and nature of personal data in relation to each individual natural person director is set out above.

*Does the proposal involve new or significantly different handling of personal data about a large number of individuals?*

**No.**

We cannot yet be clear how many new individual natural person directors might be registered in response to the policy change.

In response to changes to restrict the use of corporate directors, we know there are 67,000<sup>27</sup> companies acting as corporate directors and the moment and 102,000 individual corporate directorships. Some might be in scope of exceptions, some might not replace their corporate director with a natural person, others might use an individual natural person director who is already a director and on whom information is already available.

In response to changes to increase the accountability of those who control a single company director, we have some indication of directors who have multiple directorships and might be being controlled, but we do not know how many controlling arrangements there are overall, nor how many will react to the change.

*Does the proposal involve new or significantly different consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?*

**No.**

**Exemptions:**

*Does the proposal relate to data processing which is in any way exempt from legislative data protection measures, for example, processing of personal data for the purposes of national security?*

**No.**

*Does the proposal's justification include significant contributions to public security measures, for example, serious convicted offenders who have served their sentence and are released into the community. In these cases, personal data may need to be shared to ensure the safety of the public.*

**No.**

*Does the proposal involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable data protection regulation?*

**No.**

---

<sup>27</sup> This figures includes corporate members of LLPs.

# Director Disqualification: Privacy Impact Assessment

## What is a privacy impact assessment?

1. A privacy impact assessment is a process which helps an organisation to identify and reduce the privacy risks of a project. An organisation should use a PIA throughout the development and implementation of a project, and can use existing project management processes. A PIA enables an organisation to systematically and thoroughly analyse how a particular project or system will affect the privacy of the individuals involved.
2. The purpose of the PIA is to minimise privacy risks while meeting the aims of the project. Organisations can identify and address risks at an early stage by analysing how the proposed uses of personal information and technology will work in practice. They can test this analysis by consulting with people who will be working on, or affected by, the project.
3. Conducting a PIA is not a legal requirement of the DPA. The ICO promotes PIAs as a tool which will help organisations to comply with their DPA obligations, as well as bringing further benefits. Carrying out an effective PIA should benefit the people affected by a project and also the organisation carrying out the project.
4. More information on PIAs can be found in the [ICO's guidance document](#).

## What do we mean by privacy?

5. Privacy, in its broadest sense, is about the right of an individual to be let alone. It can take two main forms, and these can be subject to different types of intrusion:
  - Physical privacy - the ability of a person to maintain their own physical space or solitude. Intrusion can come in the form of unwelcome searches of a person's home or personal possessions, bodily searches or other interference, acts of surveillance and the taking of biometric information.
  - Informational privacy – the ability of a person to control, edit, manage and delete information about themselves and to decide how and to what extent such information is communicated to others. Intrusion can come in the form of collection of excessive personal information, disclosure of personal information without consent and misuse of such information. It can include the collection of information through the surveillance or monitoring of how people act in public or private spaces and through the monitoring of communications whether by post, phone or online. It extends to monitoring the records of senders and recipients as well as the content of messages.

## Objective

6. The objective of conducting this PIA is to identify any data protection issues in relation to the Director Disqualification section of the Transparency and Trust package. The PIA will identify any potential privacy risks and focus on whether the policy complies with the Data Protection Act and other relevant legislation.

## PIA Process

7. The screening process for this PIA was conducted in accordance with the ICO guidance in August 2010, as this was the most current document when the screening processes were commissioned. This guidance is attached.
8. The PIA process is a flexible one, and an organisation can integrate it with their existing approach to managing projects. The ICO's handbook suggests undergoing a screening process to determine the key data protection and security issues of a particular proposal. The responses to these questions will indicate whether a full scale PIA is required, or if a small scale assessment is sufficient. The process for undertaking both assessments is the same, but the level of detail is different. To perform a PIA adequately, Government officials are advised to work their way through both sets of questions.

## Step 1 – Criteria for full scale PIA

9. The first part of the screening process is a series of 11 questions focusing on issues including technology, identity, multiple organisations, data, exemptions and exceptions. The answers to the questions need to be considered as a whole to decide whether the overall impact and the related risk warrant a full scale PIA.

## Step 2 – Criteria for small scale PIA

10. These questions should be considered to determine whether a small scale PIA is required.
11. If the results of both sets of screening questions suggest that a PIA is not required, then a check will still be required to ensure that the policy or project meets the requirements of the DPA. These Data Protection Principles are outlined below:

## Data Protection Principles

12. The DPA regulates the processing of personal data through an enforceable set of good practice handling rules known as the data protection principles.

13. The eight data protection principles are expressed in general terms, and state that personal data must be:

- Fairly and lawfully processed;
- Processed for specific and lawful purposes and not further processed in a way that is incompatible with the original purpose;
- Adequate, relevant and not excessive;
- Accurate and up to date;
- Not kept for longer than is necessary;
- Processed in accordance with the data subject's rights;
- Kept secure;
- Not transferred to countries outside the European Economic Area unless an adequate level of protection is ensured or an exemption applies.

## Objectives of the policy

14. Proposed Amendments:

- Broaden the matters a Court or the Secretary of State must have regard to when deciding whether or not to disqualify, or accept a disqualification undertaking from, a director.
- Increasing the time limit within which disqualification proceedings must be taken following the insolvency of a company.
- Remove legislative barriers making it easier to bring disqualification proceedings on the basis of information provided by regulators and third parties.
- Enable director disqualification proceedings to be taken in the UK against a person who has been convicted of a serious company-related offence overseas.
- Allow compensation orders to be made against, or compensation undertakings to be accepted from disqualified directors to compensate creditors who have suffered loss as a result of their misconduct.
- Aligning bankruptcy and debt relief restrictions across the UK.

15. Measures relating to those who control directors are covered in a separate PIA.

## Overview of Disqualification

16. The Company Directors Disqualification Act 1986 (CDDA) aims to maintain the integrity of the business environment. Those who become directors of limited companies should:

- Carry out their duties with responsibility; and
- Exercise adequate skill and care with proper regard to the interests of the company, its creditors and employees.

17. The majority of directors do this effectively, but the CDDA is a powerful tool against those who abuse the privilege of limited liability. The CDDA applies not just to persons who are formally appointed as directors but to those who carry out the functions of directors.
18. Disqualification proceedings are generally brought by The Insolvency Service on behalf of the Secretary of State or, in compulsory winding-up cases, by the official receiver at the direction of the Secretary of State. The matter is heard, and decided by the court, unless the Secretary of State accepts a disqualification undertaking from a director. An undertaking has the same legal effect as a court order, but negates the need to go to court.
19. If a company director is disqualified (by court order or by giving an undertaking), unless they have court permission to act in the management of a company, that person is disqualified for the period stated in the order or undertaking from:
- Being a director of a company;
  - Acting as receiver of a company's property;
  - Directly or indirectly being concerned or taking part in the promotion, formation or management of a company;
  - Being a member of or being concerned or taking part in the promotion, formation or management of a limited liability partnership; or
  - Acting as an insolvency practitioner (IP).

## **Policy 1: Broaden the matters a Court or the Secretary of State must have regard to when deciding whether or not to disqualify a director.**

### ***The issues and goals of the policy***

20. When determining whether a director is unfit, the court must take account of matters set out in Schedule 1 to the CDDA. The Secretary of State must have regard to the same matters when deciding whether to accept an offer of an undertaking.
21. Although both legislation and case law have moved on since the enactment of the CDDA, there have been no substantive amendments to Schedule 1, giving rise to the question as to whether it is now fit for purpose and, in particular, is transparent about the breadth of misconduct that might lead to disqualification proceedings.
22. It is proposed to revise or rewrite Schedule 1 to render it fit for purpose for the present day, to make it clear to directors the wide range of misconduct that may



lead to disqualification and to address perceptions that not all relevant matters of public interest are taken into account.

***What does the policy set out to achieve?***

23. The proposed amendments to Schedule 1 are intended to deliver greater certainty and transparency as to the conduct that may result in disqualification action by setting out comprehensively and in broader, more generic, terms the matters that the court or the Secretary of State must (as opposed to may) take into account in determining unfitness and also to mandate the civil court to consider the matters concerning unfitness in deciding whether and for how long to disqualify an individual, even when a determination of unfitness is not a requirement for a disqualification order.
24. A greater level of certainty of what factors must be taken into account by the court or the Secretary of State would also assist a director who is facing disqualification proceedings to make the decision as to whether to resist such proceedings or to settle them by means of undertaking.

***Who is affected by the policy?***

25. All directors of companies, including, , who will have better transparency as to what conduct might render them vulnerable to disqualification proceedings under the CDDA; and
26. All Insolvency Practitioners who both advise and must report upon the conduct of directors of companies which enter insolvency proceedings.

## **Policy 2: Increasing the Time Limit within which Disqualification Proceedings following the Insolvency of a Company**

***The issues and goals of the policy***

27. Current law requires The Insolvency Service to commence (issue) company director disqualification proceedings within two years of the date of the insolvency when a disqualification is being taken under section 6 CDDA. In the majority of cases the current time limit is sufficient. However because investigations cannot begin until the insolvency practitioner (IP) has reported, more time may be required in a large or complex case, or one where the IP has discovered evidence late in the day. The Insolvency Service can apply to the Court for leave to commence proceedings out of time, to gain additional investigation time, but it is only granted in exceptional circumstances.
28. Further, if investigations have concluded and pre-issue negotiations with a defendant are protracted, proceedings must be issued 'protectively' in order not

to breach the statutory time limit – thereby incurring otherwise unnecessary legal costs and increasing pressure on the director involved.

29. It is therefore proposed to increase the time limit for issuing the proceedings to three years from the date of the insolvency. The overarching policy objective is to ensure that The Insolvency Service on behalf of the Secretary of State has sufficient opportunity to bring disqualification proceedings in circumstances where it is in the public interest to do so. The intention is to allow additional time for investigation in large or complex cases, to allow greater scope to consider 'late' evidence and to reduce the need for The Insolvency Service to issue proceedings protectively, which imposes some costs.

***What does the policy set out to achieve?***

30. Although it is envisaged that the vast majority of cases would continue to be brought within two years, expanding the limitation period to three years would allow deserving cases where the evidence is provided very late or the failure is so large or complex that the investigation itself takes longer than the norm. It might also remove the barrier to notifying late recovered information to The Insolvency Service by an IP who may have the perception that it is too late to report new evidence at a late stage.
31. In 2013-14 the average length of time from insolvency date to a disqualification undertaking being accepted from a director was just under 2 years. Negotiations between directors and those acting for the Secretary of State in relation to the offer of a disqualification undertaking can be protracted and the current two-year limit can result in proceedings needing to be issued at court merely to meet that time limit, at some cost to both parties (especially the directors who will be pursued for the legal costs where they offer an undertaking after proceedings are issued). Extending that time limit to three years will remove that need and therefore that cost in many cases.

***Who is affected by the policy?***

32. All directors of companies which have entered insolvency proceedings, who will be exposed to the risk of disqualification proceedings for an additional year; and all Insolvency Practitioners who must report upon the conduct of directors of companies which enter insolvency proceedings.

## **Policy 3: Enhancing the Ability to use Third Party Information as a basis of Disqualification Action**

***The issues and goals of the policy***

33. Other than in certain narrow circumstances, only The Insolvency Service, acting on behalf of the Secretary of State, has the power to institute company director

disqualification proceedings. Other regulators, including government departments and sectoral regulators, who consider that disqualification action is merited will, often at the conclusion of their own enquiries, need to refer the matter to The Insolvency Service, which may take disqualification action on the basis of 'investigative material'. However, as currently drafted, the legal definition of 'investigative material' for this purpose is so restrictive as to often require The Insolvency Service to undertake a separate investigation, duplicating some enquiries already made in order to be able to take disqualification action and unnecessarily incurring additional cost.

34. It is proposed to amend section 8 of the CDDA to widen the definition of 'investigative material', on which The Insolvency Service could rely to bring disqualification proceedings against an individual, following referral from another regulator.

***What does the policy set out to achieve?***

35. The amendment to the legislation is intended to ensure that unacceptable conduct by company directors across the UK economy and particularly in key sectors is tackled expeditiously and using the best possible information.
36. The change proposed to the CDDA is aimed at ensuring that, where directors commit serious breaches of sectoral rules and regulations, reports and information provided by regulators and others can be used by those acting on behalf of the Secretary of State to decide whether or not to issue disqualification proceedings against directors of companies in those sectors.
37. This will result in a more efficient and co-ordinated approach to company investigations, removing the need that can arise currently of the Insolvency Service needing to make enquiries to obtain information which is already in the hands of other regulators, but which cannot be used in the form it has been provided as a basis for taking action.

***Who is affected by the policy?***

38. All directors of companies, including, particularly directors of companies in regulated sectors; and
39. All Insolvency Practitioners, who must report upon the conduct of directors of companies which enter insolvency proceedings.

## **Policy 4: Enable director disqualification proceedings to be taken in the UK against a person who has been convicted of a company-related offence overseas**

### ***The issues and goals of the policy***

40. A person convicted of an offence in the UK in connection with the promotion, formation or management of a company may be disqualified for up to 15 years by the criminal court, or separate civil proceedings can be taken on behalf of the Secretary of State on the basis of the conviction.
41. However, there is no provision in UK law that would enable disqualification proceedings to be taken against a person who has been convicted of an equivalent criminal offence overseas. Ministers wish to rectify that to remove the risk of such person causing harm to UK businesses and consumers.

### ***What does the policy set out to achieve?***

42. The policy will enable a civil application to be made to court on behalf of the Secretary of State on the basis of the overseas conviction for an order disqualifying the individual from acting in the management of a company for a period of anything up to 15 years.
43. The order would have the same standing as any other disqualification order made by a court in the UK meaning that the individual would be unable to act in the management of a company without permission from the court.

### ***Who is affected by the policy?***

44. Directors who have been convicted of an offence in connection with the management of a company overseas; and
45. Members of the business community and consumers in the UK who will benefit from the additional protection the measure will provide.

## **Policy 5: Increase the likelihood of directors compensating creditors who have suffered loss as a result of their misconduct.**

### ***The issues and goals of the policy***

46. Insolvency and company law strikes a balance by allowing individuals to trade with the benefit of limited liability, thereby encouraging entrepreneurs and responsible risk taking, whilst at the same time placing duties on directors to ensure they take their obligations seriously.

47. To deal with the minority of directors who wilfully or recklessly fall short of those standards, provisions exist to enable action to be taken in the public interest to bar individuals from acting in the management of companies and ensure creditors have an opportunity get financial redress for resulting losses.
48. Those mechanisms do not work as effectively or transparently as the Government desires. It is therefore proposed to strengthen the protections to increase the likelihood of creditors being compensated in appropriate cases, whilst not posing any additional risk to the great majority of directors who play by the rules.

***What does the policy set out to achieve?***

49. The policy is intended to strengthen mechanisms that already exist to protect creditors by:-
- Enabling a Compensation Award to be made against a director who has been disqualified as a director where the conduct for which they have been disqualified has caused loss to creditor(s) of an insolvent company; and
  - Allowing certain civil actions that can already be taken against directors by liquidators and administrators to remedy improper actions to be capable of being assigned to creditors and other third parties to pursue.

***Who is affected by the policy?***

50. Creditors of insolvent companies who have suffered loss arising from misconduct by directors.
51. The 1200-odd directors who are disqualified each year having been found to be unfit to act in the management of companies and any other directors who have breached their duties as directors;
52. Legal professionals who provide advice to directors of companies facing financial difficulties and possible insolvency and to those directors who are facing disqualification proceedings.

## **Policy 6: Aligning bankruptcy and debt relief restrictions across the UK**

***The issues and goals of the policy***

53. When an individual is unable to pay his debts as they become due, the individual or one of their creditors may apply to the court for a bankruptcy order to be made. For those in need of debt relief but with very limited assets and very low income, debt relief orders are available as an alternative to bankruptcy. Bankruptcy and debt relief impose certain restrictions on an individual, which can be extended for a period of between two to 15 years if the individual is found to have acted

dishonestly or found to be blameworthy in relation to their financial affairs. The restrictions prohibit an individual from acting as a director of a company and also disqualify an individual from acting as an insolvency practitioner.

54. Devolved administrations have separate legislation which governs insolvency. The different application of bankruptcy restrictions across the UK has resulted in uncertainty as to whether equivalent legislation on bankruptcy and debt relief restrictions can be reciprocated. So, for example, while an undischarged bankrupt in Great Britain cannot act as a company director in Great Britain, the same individual may be able to go to Northern Ireland and act as a company director. Conversely, an individual subject to bankruptcy restrictions in Northern Ireland may be able to come to England and Wales and be a company director while banned from doing so in Northern Ireland.

***What does the policy set out to achieve?***

55. The amendment to the policy is a technical one which is intended to change the necessary primary legislation in Great Britain and Northern Ireland. The change will provide reciprocal recognition across GB and Northern Ireland which will ensure automatic disqualification of individuals as company directors and insolvency practitioners in other UK jurisdictions once they are subject to statutory bankruptcy or debt relief restrictions.

***Who is affected by the policy?***

56. All undischarged bankrupts and individuals subject to debt relief orders.
57. All individuals who are subject to bankruptcy restrictions either as undischarged bankrupts, have bankruptcy restrictions orders and undertakings (the administrative version of bankruptcy orders), debt relief orders, debt relief restriction orders undertakings.
58. All directors of companies once they are subject to bankruptcy or debt relief restrictions as directors would be required to step down from their directorship.
59. Legal and insolvency professionals who provide advice to directors.
60. Legal professionals who provide advice to individuals who have been made bankrupt or who are about to be made bankrupt.

***Impact***

61. We have completed the required screening process for these policies and are satisfied that a PIA does not need to be completed. The screening assessment at Annexes A and B covers the proposals to strengthen the disqualification framework, financial redress mechanisms and minor and technical amendments around bankruptcy restrictions applying throughout the UK, arising from the Transparency and Trust discussion paper to be contained in primary legislation

(matters of unfitness, overseas conduct, time periods, legislative gateways, compensation awards, assigning actions, bankruptcy restrictions).

62. Where the screening process identified a risk around data handling, this risk can be shown to have been mitigated by the fact that it is information currently received from other regulators, e.g. FCA. There is nothing new in terms of data collection/retention.

63. We are confident that the policy meets the data protection principles outlined above.

## Annex A: Screening process for a small scale PIA

### Technology:

*Does the proposal involve new technologies or technologies that can substantially reveal personal information, such as visual surveillance, digital image and video recording?*

**No.**

### Justification:

*Is the justification for the new data-handling unclear or unpublished?*

**No.**

### Identity:

*Does the proposal involve an additional use of an existing identifier?*

**No.**

*Does the proposal involve use of a new identifier for multiple purposes?*

**No.**

*Does the proposal involve new or substantially changed identity authentication requirements that may seek excessive personal information or be onerous upon an individual? It is important that identity authentication is proportionate to the purpose. For example, in some situations face to face contact may have a lower threshold for identity authentication while electronic transactions may have a higher threshold of authentication and may seek more than one assurance.*

**No.**

### Data:

*Will the proposal result in the handling of a significant amount of new personal data about each person, or significant change in existing data-holdings?*

**No.**

*Will the proposal result in the handling of new personal data about a significant number of people or a significant change in the population coverage?*

**No.**



*Does the proposal involve new linkage of personal data with data in other collections, or significant change in data linkages?*

**No.**

**Data handling:**

*Does the proposal involve new or different data collection policies or practices that may be unclear or seek excessive information that is not relevant to the purpose? Data controllers should seek to identify the minimum amount of information that is required in order properly to fulfil their purpose. Processing excessive amounts of information that is not required for the purposes of the data controller will be in breach of the data protection principles.*

**No.**

*Does the proposal involve new or different data quality assurance processes and standards that may be unclear or unsatisfactory?*

**No.**

*Does the proposal involve new or different data security arrangements that may be unclear or unsatisfactory?*

**No.**

*Does the proposal involve new or different data access or disclosure arrangements that may be unclear or permissive?*

**No.**

*Does the proposal involve new or different data retention arrangements that may be unclear or extensive?*

**No.**

*Does the proposal involve changing the medium of disclosure for publicly available information in such a way that the data becomes more readily accessible than before?*

**No.**

**Exceptions:**

*Will the proposal give rise to new or changed data-handling that is in any way exempt from legislative data protection measures? This could include, for example, national security information systems.*

**No.**

## Annex B: Screening process for a full scale PIA

### Technology:

*Does the proposal apply new or additional information technologies that could affect an individual such as locator technologies (including mobile phone location)?*

**No.**

### Identity:

*Does the proposal involve new identifiers or re-use of existing identifiers, such as digital signatures?*

**No.**

*Might the proposal have the effect of denying anonymity and pseudonymity, or converting transactions that could previously be conducted anonymously or pseudonymously into identified transactions?*

**No.**

### Multiple Organisations:

*Does the proposal involve multiple organisations, whether they are Government agencies (for example in “joined-up Government” initiatives) or private sector organisations (for example, as outsourced service providers or as “business partners”)?*

**Partly.**

Whilst gateways do concern our use of information, it is information we currently receive from other regulators, e.g. FCA. There is nothing new in terms of data collection/retention etc. We currently receive data and have to re-collect it as the data doesn't meet our definitions of what can be adduced into court as a DQ. The change saves us re-collecting the same data as we will be able to adduce the data that we currently receive through normal channels.

### Data:

*Does the proposal involve new or significantly different handling of personal data that may be of particular concern to individuals?*

**No.**

*Does the proposal involve new or significantly different handling of a considerable amount of personal data about each individual in the database?*

**No.**

*Does the proposal involve new or significantly different handling of personal data about a large number of individuals?*

**No.**

*Does the proposal involve new or significantly different consolidation, inter-linking, cross-referencing or matching of personal data from multiple sources?*

**No.**

**Exemptions:**

*Does the proposal relate to data processing which is in any way exempt from legislative data protection measures, for example, processing of personal data for the purposes of national security?*

**No.**

*Does the proposal's justification include significant contributions to public security measures, for example, serious convicted offenders who have served their sentence and are released into the community. In these cases, personal data may need to be shared to ensure the safety of the public.*

**No.**

*Does the proposal involve systematic disclosure of personal data to, or access by, third parties that are not subject to comparable data protection regulation?*

**No.**

© Crown copyright 2014

You may re-use this information (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence. Visit [www.nationalarchives.gov.uk/doc/open-government-licence](http://www.nationalarchives.gov.uk/doc/open-government-licence), write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: [psi@nationalarchives.gsi.gov.uk](mailto:psi@nationalarchives.gsi.gov.uk).

This publication available from [www.gov.uk/bis](http://www.gov.uk/bis)

Any enquiries regarding this publication should be sent to:

Department for Business, Innovation and Skills  
1 Victoria Street  
London SW1H 0ET  
Tel: 020 7215 5000

If you require this publication in an alternative format, email [enquiries@bis.gsi.gov.uk](mailto:enquiries@bis.gsi.gov.uk), or call 020 7215 5000.

**BIS/14/884**