Department for Business Innovation & Skills

COMPANY FILING REQUIREMENTS- RED TAPE CHALLENGE

Company Filing Requirements: Privacy Impact Assessment

JUNE 2014

Contents

Introduction

The following document includes the Privacy Impact Assessment (PIA) for the company filing measures included in Part 8 of the Small Business, Enterprise and Employment (SBEE) Bill ('Company Filing Requirements').

The screening process found that a full PIA was not required.

Background

The proposals on company filing requirements come out of the Company and Commercial Law Red Tape Challenge. They were part of the Red Tape Challenge consultation (in January and February 2012) and were subsequently consulted on in October and November 2013. No concerns were raised by respondents about any adverse impact on privacy as a result of the proposals.

The objectives of the package of deregulatory proposals on company filing requirements are to:

- Improve and simplify the current requirements for companies to file certain information on the UK company register;
- Improve the quality of the information on the UK company register; and
- Make identity theft more difficult.

The formal government response to the discussion paper was published in April 2014. The response set out the package of reforms to be taken forward.

More detail about the policy can be found in the text below.

Privacy Impact Assessments

The PIA in this document has been conducted in order to identify any data protection issues in relation to the company filing requirements policy. The PIA has identified any potential privacy risks and focus on ensuring that the policy complies with the Data Protection Act 1998 (DPA) and other relevant legislation.

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.

The document will be updated in light of any changes made to the policy which may have an impact on privacy. The PIA below is current as of June 2014.

Please contact the Transparency and Trust team at the Department for Business, Innovation and Skills (transparencyandtrust@bis.gsi.gov.uk) if you require more information.

Company Filing Requirements: Privacy Impact Assessment

What is a privacy impact assessment?

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.

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.

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.

More information on PIAs can be found in the ICO's guidance document.

What do we mean by privacy?

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 of the Privacy Impact Assessment

The objective of conducting this PIA is to identify any data protection issues in relation to the company filing requirements 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

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.

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

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

These questions should be considered to determine whether a small scale PIA is required.

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

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

The proposals on company filing requirements come out of the Company and Commercial Law Red Tape Challenge. They were part of the Red Tape Challenge consultation (in January and February 2012) and were subsequently consulted on in October and November 2013. No concerns were raised by respondents about any adverse impact on equality as a result of the proposals.

The objectives of the package of deregulatory proposals on company filing requirements are to:

- Improve and simplify the current requirements for companies to file certain information on the UK company register;
- Improve the quality of the information on the UK company register; and
- Make identity theft more difficult.

Who is affected by this policy?

The proposed policies will affect companies registered in the UK, regardless of who the directors or owners (members) of that company are. A company is legally distinct from the people who own and run them. However, the provisions relate to the filing of information with the registrar of companies, which may include information about the directors and the members.

Main difference between the new policies and the current position

New Policy	Current position
Annual return	
Companies will be required to check and confirm their information via a tick box approach at least once in any twelve month period, rather than a set point in the year. If a company updates its information, it can check and confirm the information at the same time.	All companies must complete a return containing basic company information at a set point each year, regardless of whether or not the information has changed in the year.

Company registers	
Private companies will be allowed to opt out of the requirement to keep the company registers and, instead, keep the information on the public register.	All companies must keep registers of directors, directors' residential addresses, secretaries and members at their registered office or an alternative location.
Statement of Capital	
Simplify the financial information contained in statements of capital.	All companies with share capital must produce a snapshot of their capital at particular points in time.
Appointment of directors and disputes	
Replace the current directors' "consent to act" filing requirement with a statement by the company that the director has consented to act, and providing a means of removing a director from the register in the event of a dispute with the company over their appointment without going to court.	Companies which appoint a new director must file a "consent to act" on the public register. Where a company objects to the removal of a director's appointment from the public register, the removal can only be affected by the court.
Directors' date of birth	
Suppress the day of director's dates of birth available for inspection on the public register.	A director's full date of birth must be available on the public register.
Fast track dissolution	
A faster "strike off" regime to get companies off the public register, whilst still giving time for creditors to object. The new process would allow the registrar to strike off companies within approximately 3 or 4 months.	Companies that are neither carrying on business nor in operation can be struck off the public register by the registrar. This process usually takes approximately 6 months.
Registered offices	
Make it simpler to object to the use of, and provide a process for the removal from the public register of, registered office addresses which companies are not authorised to use.	The circumstances in which a person may object to the use of, and apply for the removal from the public register of, a registered office address by a company is limited.
Optional information	
Allow those companies who wish to, to make additional information available on the public register if they choose to do so.	The amount of more detailed information (above the statutory minimum requirements) which a company can put on the public register is limited.

Impact

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 filing proposals to be contained in primary legislation (annual return; company registers; directors' dates of birth; statements of capital; additional information; registered office addresses; director disputes; and accelerated strike off).
Where the screening process has identified risks around data handling, these risks can be shown to have been mitigated by the following:

- putting the register of members on the public register is optional for companies; it will not be a requirement;
- as a safeguard, this option can only be exercised with the unanimous assent of members; and
- the addresses of members are already potentially available as the register of members can be inspected on request.

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?

Possibly.

Where a company takes advantage of the option to hold its register of members on the public register, this will mean that the addresses of its members will be available on the public register. However, we do not consider that this would have a significant impact on an individual's privacy for the following reasons:

- Putting the register of members on the public register is optional for companies; it will not be a requirement; and
- as a safeguard, this option can only be exercised with the unanimous assent of members.

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")?

No.

Data:

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

Possibly.

Where a company takes advantage of the option to hold its register of members on the public register, this will mean that the addresses of its members will be available on the public register. However, we do not consider that this would have a significant impact on an individual's privacy for a number of reasons:

- putting the register of members on the public register is optional for companies; it will not be a requirement;
- as a safeguard, this option can only be exercised with the unanimous assent of members; and

- the addresses of members are already potentially available as the register of members can be inspected on request.

Where a company takes advantage of the option to hold its register of directors on the public register, this will mean that the directors' full dates of birth will be available on the public register. (Under a separate proposal, part of a director's date of birth will be suppressed from the public register.) However, we do not consider that this would have a significant impact on an individual's privacy for the following reasons:

- putting the register of directors on the public register is optional for companies; it will not be a requirement;
- it will be for the directors to exercise the option; and
- the full date of birth of directors is currently available on the public register.

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.

This publication available from 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, or call 020 7215 5000.
BIS/14/888