About the Shareholder's Rights Directive and its impacts on intermediaries who now need to disclose Shareholder Identity

About the Shareholder's Rights Directive and its impacts on intermediaries who now need to disclose Shareholder Identity

Background

SRD2 updates the Directive 2007/36/EC establishing requirements in relation to the exercise of rights attached to voting shares of companies in regulated EU markets. It was a response to the financial crisis which revealed that shareholders in many cases supported their advisors' excessive short-term risk taking and poor levels of 'monitoring' of, and engagement with, investee companies.

This fact sheet provides information about the Shareholder Identification Disclosure component of SRD2 and the obligations for disclosure that Instant Actions can help you to address.

Identifying Shareholders

Because shares of listed companies are often held through complex chains of intermediaries, it can be difficult for companies to identify their shareholders, which is a prerequisite for direct communication and the exercise of rights between the shareholders and the company, particularly in cross-border situations. Under SRD2, listed companies now have the right to identify their shareholders in order to be able to communicate with them directly. Upon the request of the company, intermediaries must send shareholder identities to the requesting companies, with the exception of shareholders holding only a small number of shares. The data must include the name and contact details of the shareholder, including registration number or LEI if a legal person, and the number and classes of shares held by the shareholder and the date of their acquisition.

Why is this significant?

With regard to the directive and the reasons for its introduction, identifying shareholder identity seems a very reasonable requirement, in fact this requirement already exists in the UK under the 2006 Companies Act. However, when you consider the way shares are held, the personal data that needs to be completed, the potential conflict of both disclosing and protecting personal data and the very real confidential nature of holdings (which can move the price of shares), disclosing identity is anything but insignificant.

Who owns a company is valuable information. Plenty of stock traders watch the activity of company insiders and major institutional shareholders. Investment banks have thrived on intermediating information about shareholders. Securities borrowing desks depend on brokers knowing who owns what so they can source the stock. Which is why the well-informed pore over stock ownership disclosure forms, looking for information on which to trade. So it will not be surprising in future if

unauthorised phishing becomes prevalent on the back of ostensibly legitimate requests for shareholder identity disclosure.

Cyber Risk and Phishing

SRD2 requires firms to respond with shareholder data within 24 hours, an impossibly short time to validate that the request has come from a legitimate source, particularly when the request has not therefore come direct from the original issuer (SRD2 states that an intermediary should forward a Shareholder Identification Request to the next intermediary in the chain where necessary). As a result, the best a custodian can do is to check with the firm above them in the chain of communication that they have carried out their own validation checks. What happens if the data is inadvertently disclosed? Whose fault will it be? How will disputes be resolved? SRD2 makes reference to 'appropriate' security and that firms should check the request has come from the issuer, but does not explain how, and nor does it recognize that such a seismic change in industry workflows might require secure counter-party communications that simply don't exist today.

Validating the source of the original request – SRD2 Minimum Security Requirements

This cyber risk and risk of phishing makes it essential for intermediaries to validate that the request has come from a legitimate source. In fact article 10 of the COMMISSION IMPLEMENTING REGULATION (EU) 2018/1212 lays down minimum requirements for intermediaries to check that a shareholder identification request originates from the issuer;

Article 10 - Minimum security requirements

1.When transmitting information to intermediaries, shareholders or third parties nominated by shareholders pursuant to Articles 3a, 3b and 3c of Directive 2007/36/EC, the issuer and the intermediary shall implement appropriate technical and organisational measures aiming at ensuring the security, integrity and authentication of the information originated by the issuer or third party initiating a corporate event. Intermediaries shall implement such measures also with respect to the transmission of information to the issuer or third party nominated by the issuer.

2.The intermediary who receives from the issuer or third party nominated by the issuer a request to disclose shareholder identity, or any other communication referred to in this Regulation, which is to be transmitted along the chain of intermediaries, or to shareholders, shall verify that the request or information transmitted originates from the issuer.

- From a cyber risk perspective, relying on the best endeavours of the institution higher up the asset servicing chain to have done this satisfactorily does not provide this assurance

- Particularly if the communication has not come via SWIFT, or there is the risk of impersonation in a phishing attempt

From the 4th September therefore, intermediaries will need to have the resource in place to satisfactorily check the origin of shareholder disclosure requests. This is far from being a simple undertaking and if you do not already have arrangements in place, this is something that Instant Actions can do for you.

The potential conflict between SRD2 and GDPR (Articles 5 & 13)

Whilst imposing a significant obligation on intermediaries to disclose shareholder identity, SRD2 also makes it an obligation for member states to apply the directive in compliance with Union data protection law and the protection of privacy as enshrined in the Charter of Fundamental Rights of the European Union. So GDPR regulations apply simultaneously to SRD2 creating a potential conflict such that intermediaries must both disclose and protect personal data at the same time.

Any processing of personal data must be undertaken in accordance with Regulation (EU) 2016/679. In particular, data should be kept accurate and up to date, the data subject should be duly informed about the processing of their personal data in accordance with this Directive and should have the right of rectification of incomplete or inaccurate data as well as right to erasure of personal data. Moreover, any transmission of information regarding shareholder identity to third-country intermediaries should comply with the requirements laid down in Regulation (EU) 2016/679 under which intermediaries are subject to all of the obligations and penalties for non-compliance as data processors.

Intermediary firms will no doubt be familiar with GDPR but may have given little thought to the problem of controlling personal data as it applies to SRD2 and shareholder identity. For the purposes of transmitting shareholder identity, Intermediaries become controllers of personal data and the recipients of this data become data processors. Both data controllers and data processors are subject to the following requirements of (EU) 2016/679 - Article 5 Paragraph 1, which states that personal data shall be:

- (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');
- (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

In particular (EU) 2016/679 - Article 5 Paragraph 2 states that the controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 above - ('accountability'). So, intermediaries will need to provide comprehensive audit trails that show they have complied, and are complying, with the regulations. Intermediaries can use Instant Actions to provide this for them.

(EU) 2016/679 Article 13 Paragraph 2 also states;

In addition to the information referred to in Paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; (SRD2 states that data will only be retained for 12 months unless other regulations apply)
- the existence of the right to request from the controller access to, and rectification or erasure of, personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

- where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with a supervisory authority;
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
- the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

How those drafting SRD2 envisaged that it would be possible for intermediaries acting as controllers to comply with these requirements once the data has been passed on to issuers remains a mystery. However **Instant Actions has incorporated features into its service that intermediaries can use to update issuers to whom they have passed on shareholder identities as necessary. It also incorporates comprehensive Codelmarked audit trails that make it simple to demonstrate compliance to the regulator.**

And does the regulation apply to the UK?

Yes. The UK has adopted the directive in its entirety so all of the rights and obligations apply equally whether in the EU or the UK and third-party states. UK Commission implementing regulation http://www.legislation.gov.uk/eur/2018/1212/adopted

What are the implications of doing nothing?

In Italy fines for breaching shareholder identity disclosure can be from €30,000 up to €5m. In France dividends could be withheld for up to 5 years and as the reader will be well-aware under GDPR, fines can be up to €400m or 4% of turnover, whichever is greater.

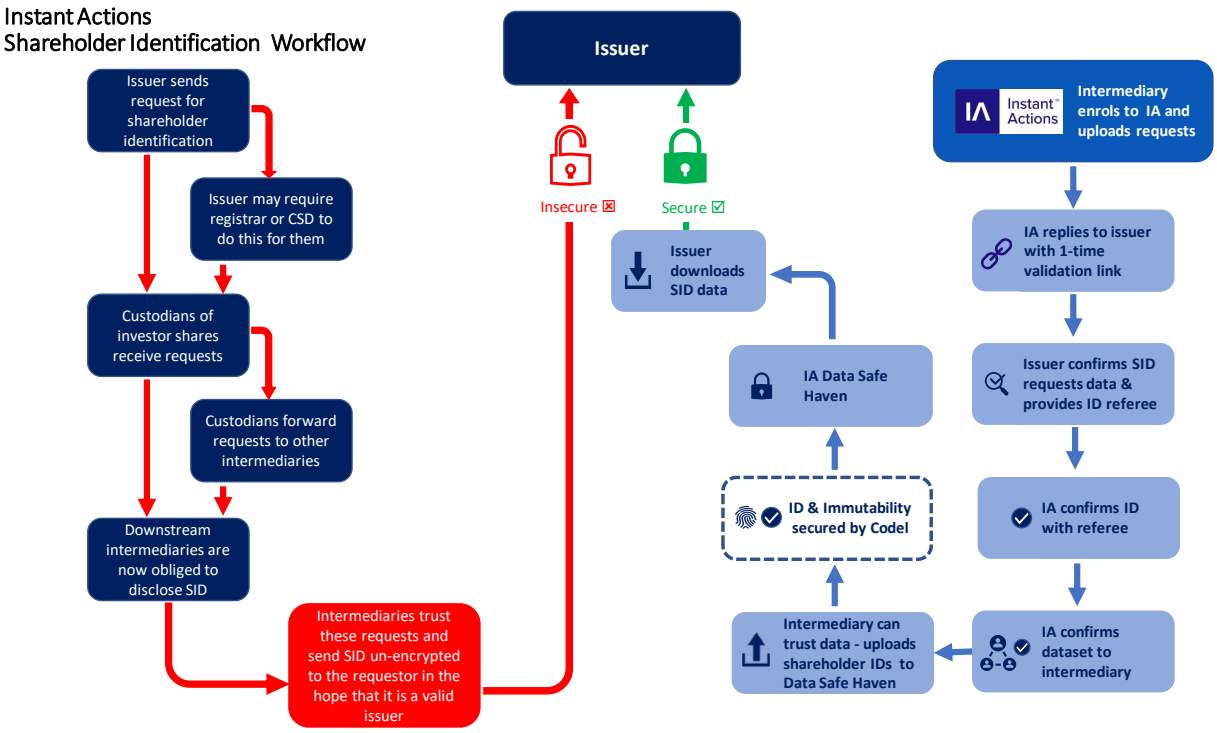
So, what can intermediaries do? How can Instant Actions Help?

Instant Actions predicts an increasing number of requests for disclosure which could turn into a deluge. It is logical to assume that for maximum transparency prior to AGMs and EGMs, all issuers will make requests twice a year – as their default position. You can also assume that intermediaries will try to cover themselves by forwarding requests to anyone who might have an investor on their books either past or present because it takes time to update the investment book of record. They might send blanket requests to any/everyone potentially resulting in hundreds of thousands of requests from multiple intermediaries. That's a huge number which will have to be dealt with manually. And then

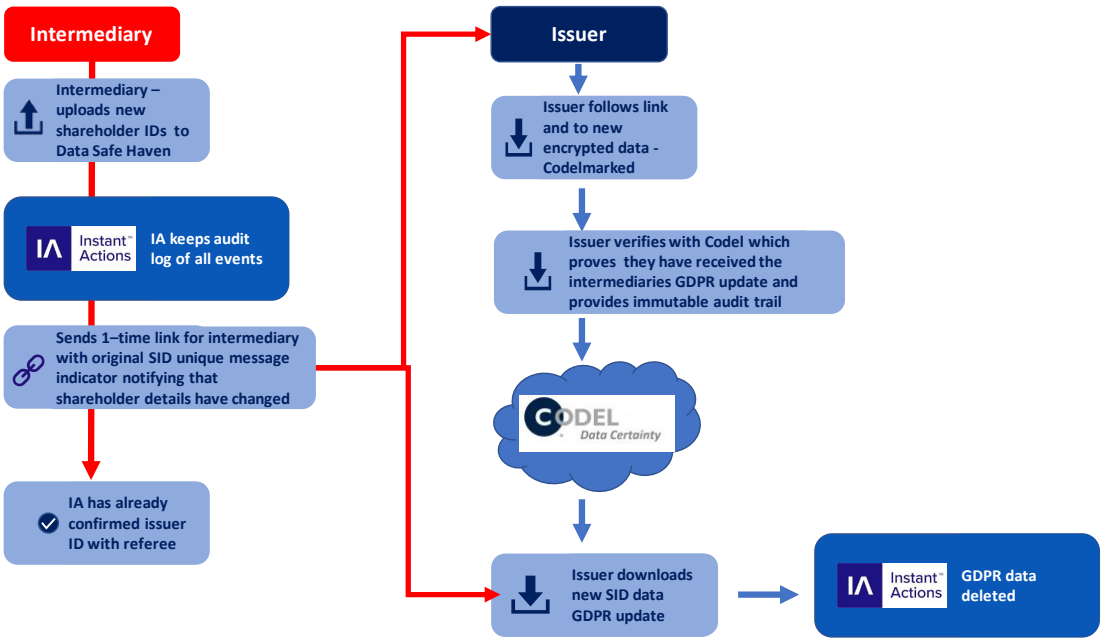
what if the regulation is extended from equities to bonds which is also on the cards – wow! Even at this early stage, some asset managers are predicting to have to manually respond to tens of thousands, perhaps hundreds of thousands, of requests annually. Translated into cost, one FTE is likely to only be able to check 15 disclosure requests per day with any reliability, so if you received 50,000 requests a year that's an extra 15 full time employees!

The following diagrams show a simple workflow available to intermediaries who want to do the following;

1. Validate that a request has originated from an issuer
2. Comply with the requirement within a 24-hour period
3. Create a data safe haven for intermediaries from which they can securely communicate shareholder identities to the issuer or their agent
4. For correction or GDPR control, update these data during the prescribed 12 months period
5. Confirm with the issuer that the data has been deleted after 12 months – the purpose for which consent has been given by the intermediary's investor client – and if not confirm the issuer's reason for retaining the data



Instant Actions
Issuer GDPR Data Compliance Workflow



For more information please contact: enquiries@instant-actions.com

Limitations

This documentation contains information that is confidential and proprietary property and/or trade secrets of Instant Actions and/or its affiliates. This documentation is not to be published, reproduced, copied, disclosed or used without the express written consent of Instant Actions. This document is provided for informational purposes only. The information contained in this document is subject to change without notice and does not constitute any form of warranty, representation, or undertaking. Nothing herein should in any way be deemed to alter the legal rights and obligations contained in agreements between Instant Actions and/or its affiliates and their clients relating to any of the products or services described herein. Nothing herein is intended to constitute legal, tax, accounting or other professional advice. Instant Actions makes no warranties whatsoever, either express or implied, as to merchantability, fitness for a particular purpose, or any other matter. Without limiting the foregoing, Instant Actions makes no

representation or warranty that any data or information supplied to or by it are complete or free from errors, omissions, or defects.