

BCR: a global data-sharing solution

24 April 2018



Building a better
working world

Overview

At EY, we believe that a strong business reputation depends on a robust data protection and information security strategy. EY views data protection and information security as fundamental components of a leading professional services organization.

We know our clients share these views, and this is why we have set out EY's approach to data protection and information security in our "Protecting your data" brochure. The present publication builds upon "Protecting your data" by outlining in more detail how EY transfers personal data internationally between the member firms, explaining our Binding Corporate Rules ("BCR") program and, of course, what this process means for our clients.

What are the legal requirements for transferring data internationally?

The international transfer of personal data is strictly regulated by European data protection law. Countries outside the European Economic Area (EEA) without a comprehensive legislative approach to data protection are not deemed by the European Union (EU) to provide an adequate level of protection for individuals' data privacy rights. Data protection law in Europe therefore prohibits the transfer of personal data to these countries, even where the importing entity is part of the same organization, unless the organization transferring the information has implemented appropriate legal safeguards.

How can EY transfer personal data on an international basis in a lawful manner?

The standard contractual clauses approved by the European Commission are used by many organizations to create the necessary safeguards. However, they are not always a suitable way of legitimizing intra-group international transfers for global, data-reliant organizations such as EY. They also do little to encourage an organization to embed data privacy compliance within the business in a meaningful, practical way.

International markets are moving faster than ever and leading organizations are globalizing rapidly. We are investing more in mobility and using our global scale to serve our clients better. Our aim, therefore, was to implement a data transfer solution that allows us maximum flexibility without excessive bureaucracy and that reinforces our commitment to effective data protection compliance.

Driven by these restrictions and our requirements, EY has adopted BCRs as the mechanism to legitimize the international transfer of personal data between EY network entities. BCRs enable us to transfer personal data seamlessly within EY network entities, facilitating borderless, cross-service-line teaming. Importantly, BCRs provide a solution in which our people, wherever they are located, are clear about their obligations when handling personal data.

In addition, our member firm in the United States has certified to the EU - U.S. and Swiss - U.S. Privacy Shield Frameworks governing transfers of personal data from the EU and Switzerland to the United States.

What are BCRs and how do they work?

BCRs are internal rules for data transfers within multinational organizations. The implementation of BCRs allow multinational organizations to transfer personal data internationally within the same organization to countries that do not provide an adequate level of protection. BCRs contain privacy principles (such as transparency, quality, security), tools of effectiveness (such as audit, training and complaint handling procedures) and an element proving that the rules are binding. Under the EU General Data Protection Regulation (GDPR), BCRs are officially recognized as a solution to legitimize internal transfers within an organization.

Organizations wishing to adopt BCRs must follow a specific authorization process. This process involves the submission of the BCR policy to the European Data Protection Authorities where the organization is located. The criteria for approval are based upon the requirements of European data protection law.

Once the BCR policy has been approved, the non-EEA entities within a multinational organization are deemed to offer adequate safeguards for the protection of the personal information transferred to them by the EEA entities within the organization. BCRs therefore strengthen local practices, empowering organizations on a global basis.

A BCR policy is, however, much more than a means of legitimizing the international transfer of personal data intra-group. BCRs introduce a 'level playing' field, enabling an organization to apply a consistent and effective approach to data protection compliance throughout the world. Ultimately BCRs contribute to the successful management and exploitation of data as a key business asset.

What do EY's BCRs mean in practice?

EY's BCR program consists of two policies: a BCR for Controller policy (BCR C) and a BCR for Processor policy (BCR P). For the majority of professional services, EY is acting as a controller, processing personal data in accordance with its own strict professional obligations. For a limited type of professional services, EY will be acting as a processor under the detailed instructions of a controller. Where EY acts as a controller, the BCR C applies; where EY acts as a processor, the BCR P applies.

At the core of the BCRs are main rules based on, and interpreted in accordance with, relevant European data protection standards. EY must follow these rules when using personal data. In summary, the rules provide that EY will:

1. First and foremost comply with local law where it exists
2. Be transparent about its uses of personal data and use personal data for a known purpose
3. Ensure data quality (for example, by keeping personal data accurate and up to date)
4. Take appropriate security measures to protect the personal data we process
5. Honor individuals' rights in relation to their personal data
6. Ensure that adequate protection is in place when personal data is transferred internationally
7. Safeguard the use of sensitive personal data
8. Allow clients to opt out of receiving direct marketing material from EY, and honor those requests (only applicable in the BCR C)
9. Protect the legitimate interests of individuals when decisions are made by automated means
10. Provide training to EY professionals who have permanent or regular access to personal data or who are involved in the collection of personal data or the development of tools used to process personal data
11. Regularly assess EY's compliance with the BCRs
12. Efficiently address complaints and questions relating to the BCRs
13. Co-operate with European data protection authorities in relation to the BCRs
14. Update European data protection authorities as required when changes are made to the BCRs
15. Take specific action when EY believes that national legislation prevents it from fulfilling its obligations under the BCRs.

Although European law applies only to personal data used and collected in the EU, we will apply the BCRs globally and in all cases where we process personal data. This global application complements our existing cohesive approach to data protection. The BCR policies bind EY network entities together in a shared standard for the use of personal data while

giving them the latitude they need to comply with their local privacy laws; help our people to understand their obligations, to collaborate and to work efficiently; and enhance our ability to provide consistent, high-quality client service worldwide, whenever and wherever we use personal data.

EY network entities have office locations in more than 150 countries. It is through the use of solutions like BCRs that we can leverage this scale and realize the benefits of our global footprint, operate more efficiently and help address our regulatory obligations.

What do EY's BCRs mean for our clients?

Our BCRs operate to legitimize the transfer of personal data from one EY network entity to another EY network entity, which will include the personal data of our clients. Our BCR P applies to data received from an EU client, acting as controller, by a non-EU EY network entity .

In terms of the benefits, our public commitment to comply with our BCRs provides legal and commercial certainty. EY people and clients have peace of mind that personal data will be treated in accordance with the high standards set out in the BCRs. This commitment, along with our ongoing respect for local data protection requirements, distinguishes EY from the competition and reinforces our commitment to achieving outstanding results. Critically, on an internal level, BCRs will help us to rationalize our information-sharing processes and remove barriers within EY, allowing us to focus on what counts: delivering excellence to our clients, globally and locally.

More information

EYs BCRs are available on ey.com/bcr.

Contact

If you have any questions on EYs BCRs, or data protection at EY, please contact us via global.data.protection@ey.com



EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2018 EYGM Limited.
All Rights Reserved.

EYG no. 02372-183GBL

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com