BMC ENHANCES PROTECTION FOR EU DATA

BMC reached an important milestone in its journey and commitment to protect customer privacy in 2015, when we became the world's first leading enterprise software solution provider to get approval from the European Union (EU) for our Data Privacy Binding Corporate Rules (BCR) both as a controller (where BMC collects data for its own benefit), and as a processor (where BMC processes data on its customers' behalf). EU BCR are considered the world's best-in-class standard of data protection to this date.

In this blog, we will discuss the additional measures BMC has put in place to keep delivering the highest level of protection to customer personal data in the context of the latest EU developments known as Schrems II.

What changed?

In July 2020, the European Court of Justice (ECJ) reminded global organizations that EU personal data needed to be protected, regardless of the location of such data, including if located in the EU, since the receiving party of such data is now of greater importance. The ECJ was specifically concerned about foreign public authorities and established the Schrems II ruling to prevent their unlawful access to EU personal data.

Organizations across the world accessing EU personal data are now required to implement further technical, organizational, and contractual measures to ensure they have an adequate level of protection.

BMC’s further commitments

To support compliance with the Schrems II ruling and prevent unlawful access to our customers’ personal data, BMC has implemented supplementary measures, which include:

- Restrictions to accessing data

BMC has a broad global distribution of personnel and data centers that allow customers to select the location of their data, dependent on their BMC offerings and services. BMC entities, all subject to the BCR, are used for general service operations such as backups, patching, and upgrades. In addition, automation is widely used, where possible, to prevent human effort.

- Data encryption

BMC offers a wide range of state-of-the-art data encryption options, both at rest and in transit, to protect data as it is stored and accessed. Decryption keys may be exclusively retained by the customer, again dependent on their BMC offerings and services.

- Customer support privacy policies

BMC supports data minimization and provides secure channels for customers to engage with BMC support resources, effectively limiting personal data sharing to that which is strictly necessary to perform our services.

- Transparency towards customers and competent authorities

According to our BCR policy and standard customer Data Processing Agreement (DPA), BMC will put any disclosure request from a public authority on hold and promptly notify the customer and the competent data protection authority. If prohibited from doing so, BMC will make its best effort, including using reasonable legal action (see below), to have the requesting body waive that prohibition. If unsuccessful, BMC will provide its competent supervisory authority with an annual report of such requests for disclosure to the extent BMC is authorized to do so.

- Challenging unlawful disclosure requests and reporting to data protection authorities

Whenever legally possible, BMC will challenge requests to disclose customer data under EU law and the laws of the requesting body, in accordance with our DPA.

This blog is provided as of the date of publication and is not to be considered as legal advice. For more details on BMC’s security and privacy positions, please visit the BMC Trust Center, check out our EU Personal Data Transfers Q&A, and contact your BMC representative.