Transform Database Recovery and Comply with GDPR

Prepare for the recovery demands of Europe’s General Data Protection Regulation (GDPR)
# Table of Contents

1 EXECUTIVE SUMMARY

2 WHAT IS GDPR?
   Focus on the Customer

   RECOVERY ASPECTS OF GDPR – FOUR MAIN REQUIREMENTS
   The Myth of Hardware Recovery Solutions
   Timely Recovery with BMC
   Proof of Recovery
   Repeatable Process
   Data Integrity

7 KEY BUILDING BLOCKS TO GDPR COMPLIANCE

CONCLUSION
Executive Summary

The European General Data Protection Regulation (GDPR) is a regulation by which the European Parliament, the Council of the European Union, and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). Unlike prior legislation, GDPR does not just demand that certain actions be performed or that recovery of data happen in a specific timeframe, but that these actions must both be provable and able to be repeatedly tested to ensure continued compliance.

This white paper explains what GDPR is, its four main requirements, and the key building blocks to GDPR compliance. BMC Recovery Solutions for DB2® and IMS™ can help achieve and demonstrate continued compliance with their unmatched recovery performance, as well as the ability to both estimate and simulate actual data recoveries.
WHAT IS GDPR?
The primary objectives of GDPR are to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. The regulation also applies to organizations based outside the EU if they collect or process personal data of EU residents. GDPR was approved and adopted by the EU Parliament in April 2016, and will take effect after a two-year transition period and will start in May 2018. According to the EU, “personal data is any information relating to an individual, whether it relates to his or her private, professional, or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or even a computer’s IP address.”

Focus on the Customer
Unlike prior regulations, GDPR focuses on the demands and needs of the customer and not the processor of the data. What this means in practice is that customer data must be protected where the customer is an EU citizen, regardless of the geographical location of the data processor. Companies that process personally identifiable data from EU citizens are required to comply with GDPR—even though they may have no physical presence in the EU themselves.

RECOVERY ASPECTS OF GDPR – FOUR MAIN REQUIREMENTS
When looking at the data recovery requirements of the GDPR legislation, there are a number of factors that need to be taken into account.

First, the data must be recoverable in a timely manner. The legislation does not define what timely means, nor does it define the nature of the failure that has led to the recovery being necessary in the first place. Therefore, companies must plan their recovery around any data loss/corruption event, especially those they cannot foresee. They must also plan for the speediest recovery possible under the circumstances. Often there is also local legislation that does mandate recovery times.

Many of the failed or only partially successful data recoveries that BMC has seen have come about when companies plan for specific kinds of events, but are then faced with something different. Although the legislation doesn’t state it specifically, it is inherent in the way that the recovery parts are phrased, that the data must be recoverable after any eventuality.

Second, what the GDPR legislation does ask though is that the “timely recovery” must be provable. It is no longer acceptable for companies to assume that everything will be all right when a recovery becomes necessary. To achieve compliance, companies have to be able to demonstrate proof that:

- The data is recoverable.
- The data is recoverable within the timeliness constraints specified.

Third, an interesting aspect of the GDPR legislation is the requirement that companies regularly demonstrate that they are still in compliance. To quote Article 32 1.(d), GDPR requires:

“A process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing...”

Fourth, it is also necessary to ensure that the integrity of personally identifiable data is ensured. This can become a particular problem where non-relational data (i.e., unstructured data) is stored in DB2® Large Object (LOB) columns. Often this data is stored for historical and perhaps compliance reasons defined by the business, such that the data is rarely read after it has been created but must be available for processing in the event it is needed.

The Myth of Hardware Recovery Solutions
Many companies mistakenly believe that their existing disaster recovery (DR) plans will be a shortcut to GDPR compliance. Unfortunately, real world experience has shown that a hardware mirror solution, which is a typical DR option, has serious drawbacks. A hardware mirror, where disk volumes are “mirrored” to a remote site, is a perfect solution to the challenge of recovery from catastrophic data loss, such as a complete power failure or significant natural event. The geographically-dispersed mirrored devices can be up and running again in a matter of hours or even minutes.

Unfortunately, the majority of recovery events are local in nature and often triggered by poor processes or personal mistakes. Any logical data loss, such as deleting the wrong data, dropping the wrong DB2 table or database or deleting the wrong IMS database, is immediately mirrored to the remote site—thus ensuring that the mirror, which is often the only source of recovery, is equally affected. In these cases, recovery of the data ends up being a manual process with a plan built on the fly to suit the situation.
This is certainly not acceptable to the requirements of GDPR and the need to be able to demonstrate timely recovery from any event. Even if companies keep a hardware mirror solution to deliver rapid offsite DR recovery, they require an alternative and flexible approach to account for local data loss/corruption. Such flexibility can only be provided by a software backup and recovery solution. Once a company has a secure backup strategy in place, a recovery from any and every eventuality is possible.

**Timely Recovery with BMC**

BMC provides market-leading tools for securing backups and performing recoveries of DB2 and IMS data. As mentioned earlier, GDPR does not just require data to be recoverable, but it has to be recovered in a timely manner. Although timely is not defined, it can be assumed that “as fast as possible” will be the guide from auditors.

Any recovery process will be constrained by the types of backups being taken. In some cases, companies are forced to compromise on their backup strategy either because increasing online availability leaves them with no room to take backups when needed or they start to take shortcuts to try and speed up the backup process. It often is not realized what impacts these shortcuts will have on a data recovery until one is needed.

BMC prides itself on delivering highly effective recovery tools for both DB2 and IMS. Over the years, improvements in performance and the addition of patented features have resulted in tools that can take backups and perform recoveries at the highest levels of performance.

It should be possible for companies to take backups of their data as and when they are needed, without looking to compromises which can adversely affect data recovery. Below is a typical benchmark of BMC Hybrid Copy technology compared with a Flash-assisted image copy provided by IBM® as part of DB2.

---

**IBM FlashCopy vs. BMC Hybrid Copy**

<table>
<thead>
<tr>
<th>Time (hh:mm)</th>
<th>DB2 V11 Elapsed</th>
<th>BMC V11.1 Elapsed</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00</td>
<td>28:48</td>
<td>36:00</td>
</tr>
<tr>
<td>00:07:12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:14:24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:21:36</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:28:48</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:36:00</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Figure 1: Elapsed Time Benchmark: IBM FlashCopy vs. BMC Hybrid Copy*
Not only is the CPU consumption significantly reduced, the elapsed time is reduced even more dramatically. This is achieved by the BMC solution choosing the most appropriate backup options at execution time, based on the size of the objects to be backed up. Other vendors, including IBM, require the same backup options be used for every DB2 table being backed up at the same time.

Speed of backups is one part of the equation, but what is also needed is timely recovery of data from those backups. It is important to note that when performing a recovery of lost or damaged production data, speed is of the essence, regardless of what any particular legislation is mandating. As attendees at a recent DB2 Mainframe Advisory Council meeting said recently, “Recovery is all about speed.”

In this example, the elapsed time for recovery has been reduced from just over fifty minutes to less than ten minutes. When considering the timeliness of a recovery in the case of GDPR, a recovery time of fifty minutes will be hard to defend as timely if it can be demonstrated that ten minutes is an achievable target.
Recovery to Current 45+ Million Rows: IBM FlashCopy vs. BMC Hybrid Copy

The improvements in recovery times for IMS databases are, in some ways, even more remarkable. See the graph below for the difference in elapsed times for IMS recovery between IBM and BMC.
Quotes from Satisfied Customers

“BMC recovered my IMS data in five hours. My previous solution took twenty-four hours.”
“With BMC, I reduced my IMS recovery time from thirty hours to only two hours.”

As with the DB2 examples, long recovery times will be hard or even impossible to defend as timely when faster options can be demonstrated.

Proof of Recovery

An aspect of GDPR that has not really been evident in legislation before is a requirement that recoverability and recovery times need to be demonstrable. It will be necessary for companies to prove to their own internal auditors or the nominated data protection officer that data recovery can be completed in the window of timeliness that has been agreed. The only accurate way to demonstrate how long it takes to complete a recovery is to actually perform one in reality.

This could take the form of a scheduled disaster recovery test, but disaster recovery (DR) is only a suitable recovery strategy for catastrophic data loss, and this is highly unlikely to be the scenario faced in reality. In addition, a DR test is incredibly resource-intensive and, in a typical business, can only be accommodated about once each year.

**BMC provides a better alternative to using the DR test to satisfy GDPR compliance.** Using simulation techniques, it becomes possible to perform a recovery of a set of DB2 or IMS objects using all the same resources as would be used in a real recovery. The only difference is that the target data is not overwritten as it would be in a real recovery situation. Using recovery simulation makes it simple to check that the achievable recovery time is still within the limits specified.

Part of recovery solutions from BMC is the concept of recovery estimation. This uses knowledge of DB2 and IMS recovery processes to calculate what the expected recovery times would be. Estimation cannot be used to define a recovery time, but it can be used as a quick guide to the estimated recovery time, without executing a full simulation. Therefore, estimation gives an indication of whether a particular recovery is still GDPR compliant. If the numbers cause alarm, a full simulation can be used to ascertain whether there is an impending issue. Estimation can also be used to perform “what if” calculations based on projected growth in data volumes or application and data complexity. This allows for advance warning that a currently compliant process may be drifting out of compliance, giving time to make the appropriate adjustments before an audit event.

Repeatable Process

GDPR also mandates that companies have “a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.” The recovery simulation from BMC makes it simple to regularly execute a trial recovery to ensure continued compliance. Because the simulation is actually running a real recovery, it is also possible to analyze how the recovery has proceeded. In many cases, it may be possible to identify bottlenecks in the process, which if removed, would allow for even faster recovery of data. Without simulation, it becomes difficult to demonstrate what the actual recovery time is likely to be, and almost impossible to fine-tune the recovery to perform at its best.

Setting up recovery jobs can be a challenge in itself. Knowledge of how backups are being taken can lead to recovery decisions that could adversely affect recovery times. **BMC’s recovery solutions include smart managers that create the optimum recovery job streams based on how backups have been taken**—thus ensuring optimum recovery speeds for particular circumstances.

Data Integrity

GDPR also mandates attention is paid to the integrity of personally identifiable data. Article 32 1.(b) of the GDPR says companies must have “the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.”

This is not typically a concern in the DB2 area, but with the advent of unstructured data being stored in DB2 large objects, the risks of data corruption and loss have increased. DB2 stores LOB data separately from the relational data to which it refers, and links the two sets of data together with internal pointers. If any of these pointers become damaged, data corruption and loss can occur. This is very different from the way DB2 stores traditional relational data.
IBM provide utilities to periodically check the integrity of LOB data (e.g., CHECK LOB, CHECK INDEX, and CHECK DATA), but customers report that running these utilities can take a significant amount of time, thus they normally don’t execute them.

Because LOB data is often not read again once it has been created, problems with the data can lie hidden until the time it is needed, at which time it is probably too late to recover it. As one of our customers said at a BMC DB2 event “We lost LOB data once. We never found out how, and we never did get it back!” This is a situation that cannot be allowed to happen under GDPR.

Fortunately, BMC has a solution in LOBMaster for DB2®, which works seamlessly with BMC NGT Reorg and NGT Utility Manager to not only reorganize LOB data, but also perform all the necessary integrity checks. Our users are finding that not only does BMC perform these checks, but the elapsed time of the LOB reorg is significantly shorter than the IBM equivalent, despite performing these integrity checks.

KEY BUILDING BLOCKS TO GDPR COMPLIANCE

According to our 2017 Mainframe Survey, we found that some of the biggest concerns around the recovery of data were:

- 27% Time taken to recover
- 15% Recovery time prediction
- 15% Proof of recoverability
- 12% Understanding recoverability

This indicates that 69% of survey respondents all have concerns about the same data recovery challenges that GDPR introduces. Each one of these concerns is addressed by BMC Recovery Solutions for DB2 and IMS.

CONCLUSION

Concerns over recovery challenges and the impending effects of GDPR are evident. GDPR is wide-reaching and will have many effects on business processes in the next few years worldwide. The full breadth and impact of the regulation has yet to be seen. However, companies should prepare themselves for the shifts in requirements sooner than later.

BMC can help give companies confidence in their recovery timeliness and estimation with the BMC Recovery Solutions for DB2 and IMS. These two solutions can provide valuable building blocks to a full GDPR solution and help prove ongoing compliance to regulators and auditors.

FOR MORE INFORMATION

To learn more, please visit Recovery Solutions for DB2 at bmc.com/it-solutions/backup-recovery-DB2 and IMS at bmc.com/it-solutions/database-management-ims.