BUSINESS OBJECTS
IN THE ERA OF GDPR
10 STEPS TO ENSURE AND MAINTAIN COMPLIANCE

EXECUTIVE SUMMARY

The General Data Protection Regulation (GDPR) challenges organizations to protect personal data of subjects in the EU. To comply with GDPR, business intelligence managers must understand the source, purpose, and location of personal data in their landscapes. As the visible part of data, Business Objects must be used to support the goals and uphold the requirements of GDPR. GB&SMITH, creator of 360Suite solutions to enhance Business Objects, developed a 10-step process to help organizations think through the challenges of GDPR compliance and take appropriate action.

WHAT IS GDPR?

By now, most people are familiar with the term GDPR, if not the intent. In short, it's a new European Union (EU) regulation (effective May 25, 2018) that governs the processing and free movement of personal data, and reflects a belief that natural persons have a fundamental right to the protection of their personal data. GDPR applies equally to organizations located in the EU and organizations outside the EU, if they offer free or paid goods or services to, or monitor the behavior of, data subjects in the EU. Organizations that fail to comply with GDPR may be fined up to €20 million or 4% of worldwide annual revenue.

WHAT IS A NATURAL PERSON?

Natural person is a legal term that means an individual human being. It distinguishes human beings from private and public organizations, which may be referred to as *legal persons*. For the purposes of GDPR, a natural person is a data subject who is within the borders of the EU when their personal data are processed. It can also be anyone, located anywhere, whose personal data are processed by a controller or processor that is established in the EU.

WHAT MAKES DATA PERSONAL?

GDPR Article 4(1) defines personal data as "any information relating to an identified or identifiable natural person." Data that makes a person identifiable, directly or indirectly, includes name, identification numbers, location data, online identifiers (e.g., internet protocol addresses, cookie identifiers, etc.), or one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity.

HOW CAN PERSONAL DATA BE PROCESSED?

Article 4(2) defines processing as "any operation . . . which is performed on personal data . . . whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." Under GDPR, all personal data are subject to the principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity,

confidentiality, and accountability. Organizations will be held accountable for collecting and using personal data only for specified, explicit, and legitimate purposes, for storing and processing personal data securely, and for deleting personal data as soon as possible.

Some kinds of personal data can't be processed at all. Article 9(1) states that the "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited" unless one of ten exceptions applies, as outlined in Article 9 (2).

WHAT QUALIFIES AS INFORMED CONSENT?

For many organizations, satisfying the lawfulness principle usually involves obtaining consent from data subjects in advance of processing personal data. Article 4(11) defines consent as "'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." For consent to be informed, the data subject should be aware of the identity of the controller and the purposes for which the personal data will be processed. Article 7(3) states that "the data subject shall have the right to withdraw his or her consent at any time" and "it shall be as easy to withdraw as to give consent."

WHAT ARE THE RIGHTS OF DATA SUBJECTS?

In addition to the right to withdraw consent, GDPR grants natural persons the following:

- Right of access by the data subject (Article 15): Right to know if a firm has their personal data and, if so, how and why the data are being processed, how long the data will be stored, and recipients of the data
- Right to rectification (Article 16): Right to correct incorrect personal data and/or complete incomplete personal data
- Right to erasure (right to be forgotten) (Article 17): Right to demand that their personal data be erased if they withdraw consent or if one of several other conditions applies
- Right to restriction of processing (Article 18): Right to restrict processing of their personal data if one of several conditions applies
- Right to data portability (Article 20): Right to receive their personal data from one controller and transmit those data to another controller
- Right to object (Article 21): Right to object to the processing of their personal data for a number of reasons, including for profiling and direct marketing
- Right to lodge a complaint with a supervisory authority (Article 13(2)(d))

WHAT ARE THE OBLIGATIONS OF CONTROLLERS AND PROCESSORS?

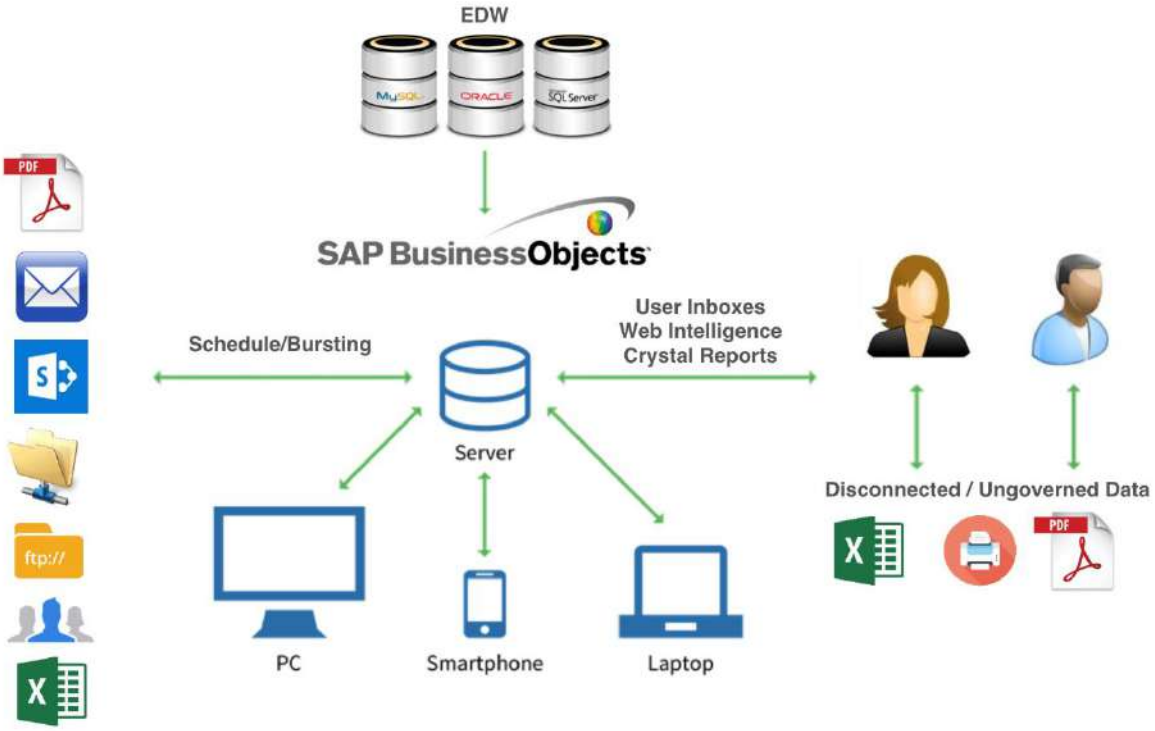
In some cases, controllers and processors are subject to the same GDPR requirements. For example, both groups must maintain records of processing activities, implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, and designate data protection officers.
But, in general, GDPR treats data controllers as the principal parties for obtaining consent and enforcing the rights of data subjects. Controllers must also notify the supervisory authority of a personal data breach within 72 hours and notify the data subject without undue delay.

To understand the distinction between controllers and processors, consider the example of UNION MANUFACTURING CO (UMC). UMC has 5,000 employees in the France, and outsources payroll, human resource, and benefits services to PAYME INC. UMC passes the personal data of UMC employees on to PAYME for processing. In this case, UMC is the controller and PAYME is the processor. UMC is responsible for obtaining personal data from employees with consent, for keeping the data up to date, including notifying PAYME of changes to personal data, and for enforcing the rights of data subjects.

HOW DOES GDPR IMPACT BUSINESS OBJECTS?

It is safe to assume that all information technology, including CRM platforms, ERP systems, and BI applications (e.g, Business Objects, Tableau, Power BI), contains personal data obtained from databases. To comply with GDPR, managers responsible for business intelligence (BI), including BI Centers of Excellence (BICOEs) and BI Competency Centers (BICCs), must be able to answer detailed questions about their landscape such as:

1. What personal data does it contain?
2. Where are personal data stored?
3. What is the lifecycle of personal data?
4. Who has access to personal data? Who uses this access?
5. How are personal data processed?
6. What safeguards are in place to secure personal data?
7. When should personal data be encrypted or pseudonymized?
8. How long are personal data retained? How can they be erased?
9. Where are the users located (e.g., in what countries)?
10. What records are kept of processing activities related to personal data?



WHAT IS 360SUITE?

360Suite by GB&SMITH is a set of software solutions including 360Eyes, 360View, 360Plus, 360Live, 360Vers, 360Scan, 360Univ, 360Bind, and 360Cast that enhance Business Objects by boosting efficiency, securing deployments, and delivering a deeper understanding of environments. Used by more than 3 million people worldwide, 360Suite helps companies and government organizations ensure that Business Objects supports policies related to governance, risk management, and regulatory compliance.

360Suite has developed a 10-step process to help organizations take appropriate technical and organizational measures to ensure that GDPR requirements are met with regard to Business Objects.

Business Objects in the Era of GDPR

10 Steps to Ensuring and Maintaining Compliance

1 Back Up Data

2 Find Personal Data

3 Tag Personal Data

4 Analyze Personal Data

5 Ensure Consistency of Personal Data

6 Ensure Traceability of Personal Data

7 Secure Personal Data

8 Permanently Rectify or Erase Personal Data

9 Monitor Use of Personal Data

10 Demonstrate Compliance with GDPR

360 Suite

SAP Partner

STEP 1: BACK UP DATA

Whether data is stored on premise, in the cloud, or both (hybrid architecture), GDPR demands a solid backup and disaster recovery plan. Article 32(1)(c) states that controllers and processors shall maintain "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident." Simply backing up Business Objects, or relying on VM or cloud backup services, is not sufficient to comply with GDPR. That's because personal data that was modified or deleted after the time of the last backup will revert to a prior state when Business Objects is restored. Also, if environments becomes corrupted, mirrored backups will be corrupted, whether on the server, VM, or cloud.

Business Objects deals in large, inflexible Business Intelligence Archive Resource (BIAR) files comprised of sets of objects. A typical Business Objects recovery strategy includes backing up the entire Business Objects server, which can restore the full system in the event of a server incident, but is not suitable for selective rollbacks, recovering a Universe, or restoring individual deleted objects. Fully restoring a Business Object environment takes time, often days.

360Plus creates one BIAR file per object and performs incremental delta and dynamic backups, which can selectively roll back to previous versions of any object at any time. By empowering organizations to restore specific content in seconds and full environments in minutes to hours, 360Suite supports continuity of operations and satisfies the GDPR requirement to restore personal data in a timely manner. [Mitigate Risks Linked to Backup, Disaster and Recovery in SAP Business Objects.]

STEP 2: FIND PERSONAL DATA

The first step toward a thorough understanding of the personal data stored in an environment is finding it and taking inventory. Locating the personal data in a Business Objects Universe is easier said than done. The Business Objects Information Design Tool (IDT) can extract data, but the tool is accessible only to IT and not to end users. 360Univ puts the power to find personal data in the hands of end users by making it possible to export Universe objects to Excel spreadsheets, which can be searched for the existence and location of personal data.

STEP 3: TAG PERSONAL DATA

After finding the personal data, tag it for reporting purposes. Article 30 states that controllers shall "maintain a record of processing activities." Article 7 states that controllers "shall be able to demonstrate that the data subject has consented to processing of his or her personal data." And Article 14(2)(f) states that, "where personal data have not been obtained from the data subject, the controller shall provide the data subject [with information about] from which source the personal data originate."

In order to create and maintain necessary records of processing activities, proof of consent, and data sources, BI managers must be able to link personal data to reporting fields. 360Univ makes it possible to tag personal data with required information, such as purposes of processing, data source, data subject category, personal data category (and sensitivity), recipient category, transfers to third

countries or international organizations, technical and organizational security measures, and time limits for erasure. Tags may vary by business unit. For example, the principle of storage limitation dictates that personal data shall not be kept for longer than necessary, which may be 6 months for a customer service department, 2 years for a support department, and 7 years for an accounting department. Tags should therefore be detailed enough to account for lifecycle differences. Highly sensitive information (e.g., health data) should be tagged for special treatment, including possible encryption or pseudonymization.

STEP 4: ANALYZE PERSONAL DATA

After tagging the personal data, the next step is to analyze it in the context of GDPR and data privacy governance rules. Is the personal data being used/not used? How is the personal data being used? How was the data obtained--directly from data subjects or from a third party? How will the data be processed? Is the processing lawful (principle of lawfulness, fairness and transparency)? Did data subjects consent to the processing of their data? Does the data include any information prohibited by Article 9 (e.g., race, ethnicity, religion, etc.)? Was the data collected for a specified, explicit and legitimate purpose (principle of purpose limitation)? Is the data relevant and limited to what is necessary for the purposes for which it is processed (principle of data minimization)? Is the data accurate and kept up to date (principle of accuracy)? Is the data kept in a form that permits identification of data subjects for no longer than is necessary (principle of storage limitation)? Is the data processed in a way that ensures appropriate security (principle of integrity and confidentiality)? Personal data that doesn't satisfy these principles has no place in an enterprise data warehouse (EDW) and should be permanently erased. 360Eyes provides insight into data usage/non-usage and 360View makes it possible to automatically delete unused data in bulk.

STEP 5: ENSURE CONSISTENCY OF PERSONAL DATA

Consistency applies not only to the actual data, but to how those data are incorporated into reports, and with whom the reports are shared. A number of 360Suite solutions support consistency. 360Bind automates regression testing to ensure the changes at the ETL, database, and Universe levels don't alter the content of reports. 360Eyes snapshots can be used to track and compare changes to security, Universes, and objects over time, and to analyze the impact on reports of changes to personal data. 360Vers can track who modified what, when, and where to reports and Universes. It also offers advanced version control with the ability to view and audit changes, secure check out, and sets up workflow approvals for traceability. rsible. It's good practice to apply version control to reports containing personal data, to be able to revert to a prior version quickly and easily as needed, and also to demonstrate GDPR compliance to the Data Protection Officer (DPO) upon request. Finally, 360View contains a delete feature that empowers Admins to delete accidentally-sent reports from user inboxes.

STEP 6: ENSURE TRACEABILITY OF PERSONAL DATA

Ensure the traceability of personal data, especially when transferring it outside an organization or outside Business Objects. GDPR (101) states that, "when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation." In other words, controllers remain responsible for the protection of personal data, obtained directly or indirectly, even after personal data is transferred. When transferring personal data from a Business Objects native format (Webi) to a non-native format (e.g., PDF, XLS), organizations should implement safeguards, such as password protecting personal data with 360Cast. When transferring personal data to a third party, organizations should ensure that data is tagged with compliance information (e.g., lifecycle), such as those created with 360Univ (see step 3). Regardless of the type of transfer, organizations should flag each and every instance of personal data, which is possible with 360Cast.

STEP 7. SECURE PERSONAL DATA

After finding, tagging, and analyzing personal data, take steps to secure access to it. GDPR states that "personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing." Article 25 specifies that "by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage, and their accessibility." Controllers are responsible for securing access to personal data obtained directly or indirectly, as well as data transferred to third parties. Organizations should also plan for malicious activity and develop a plan of action.

Personal data can be secured in different ways. Business Intelligence managers can control and recertify who has access to personal data. 360Eyes tracks and documents security over time. 360View enhances security by providing a patented comprehensive view of inherited rights and double-inherited rights. This is particularly important when processing personal data because a cascade effect is possible every time security is modified. 360View also simplifies the process of auditing and modifying security rights, and offers the possibility to perform segregation of duties (SOD).

In addition to recertifying users/access, directors of business intelligence can secure personal data by regularly recertifying accounts and retaining only essential personal data. Information is non-essential if, inter alia, it is never used or it is at the end of its lifespan. 360Eyes facilitates the recertification process by providing insight into the usage/non-usage of personal data. 360View makes it possible to delete data in bulk, including force-purging inboxes and Webis, and auto-cleaning deployments.

Another way directors of BI can secure personal data is by implementing appropriate technical measures to render personal data unintelligible (e.g., pseudonymization) or unintelligible to any person who is not authorized to access it (e.g., encryption).

STEP 8. PERMANENTLY RECTIFY OR ERASE PERSONAL DATA

Make sure that all changes to personal data are permanent, even in the event of a technical or physical incident. Fundamental to GDPR are the rights of data subjects to rectify and erase personal data. A*rticle 16* states that "the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. " *Article 17* states that "the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data." Simply rolling back to the most recent backup will lose more recent changes, including changes to personal data. Take for example, the case of an organization that last backed up Business Objects on March 1, made changes to personal data on March 2, and had a technical incident on March 3. Restoring Business Objects to the March 1 backup will lose the March 2 changes. 360Plus delta and dynamic backups, combined with 360Eyes snapshots, makes it possible to identify all changes made since the last backup and selectively roll back to previous versions of any object.

STEP 9. MONITOR USE OF PERSONAL DATA

Another way to ensure security is to monitor how personal data is used. 360Eyes makes it possible to audit actions on personal data in Business Objects, track personal data within reports, track report usage (including actions on reports), identify duplicate reports, and identify changes to Universes. 360Eyes can also identify users who accessed personal data in Business Objects, what actions they performed on the personal data, and the IP addresses of hardware from which the actions were carried out. Finally, 360Eyes can take snapshots of Business Objects over an extended period of time, which can be exported and compared to overcome auditing spaces. 360Suite doesn't use sniffers and can gather information during off-peak hours to avoid impacting production.

STEP 10: DEMONSTRATE COMPLIANCE WITH GDPR

Demonstrate compliance to quickly satisfy requests from Data Protection Officers and certification bodies. Per GDPR Article 24, organizations must be able to demonstrate that they are complying with GDPR. (The controller shall "be able to demonstrate that processing is performed in accordance with this Regulation.") 360Suite solutions, including 360Plus, 360Univ, 360View, 360Cast, 360Eyes, 360Bind and 360Vers, help organizations achieve excellence, and GDPR compliance is no exception. Not only does 360Suite help organizations process personal data in accordance with GDPR, it also provides them with the means to document compliance. In this way, 360Suite is as much a business as an IT solution, bringing both parties together in support of a shared goal--organizational success.

GLOSSARY OF TERMS

Business Intelligence
A technology-driven process for analyzing data to help end users make informed business decisions

Consent
Any freely given, specific, informed, and unambiguous agreement to the processing of personal data

Controller
Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing personal data

Data Subject
A natural person to whom personal data relates

European Union (EU)
A political union, currently comprised of 28 member nations

General Data Protection Regulation (GDPR)
A European Union regulation that aims to standardize and strengthen data protection policies for residents of EU member nations

Legal Person
An individual, company, or other entity that has legal rights and is subject to obligations

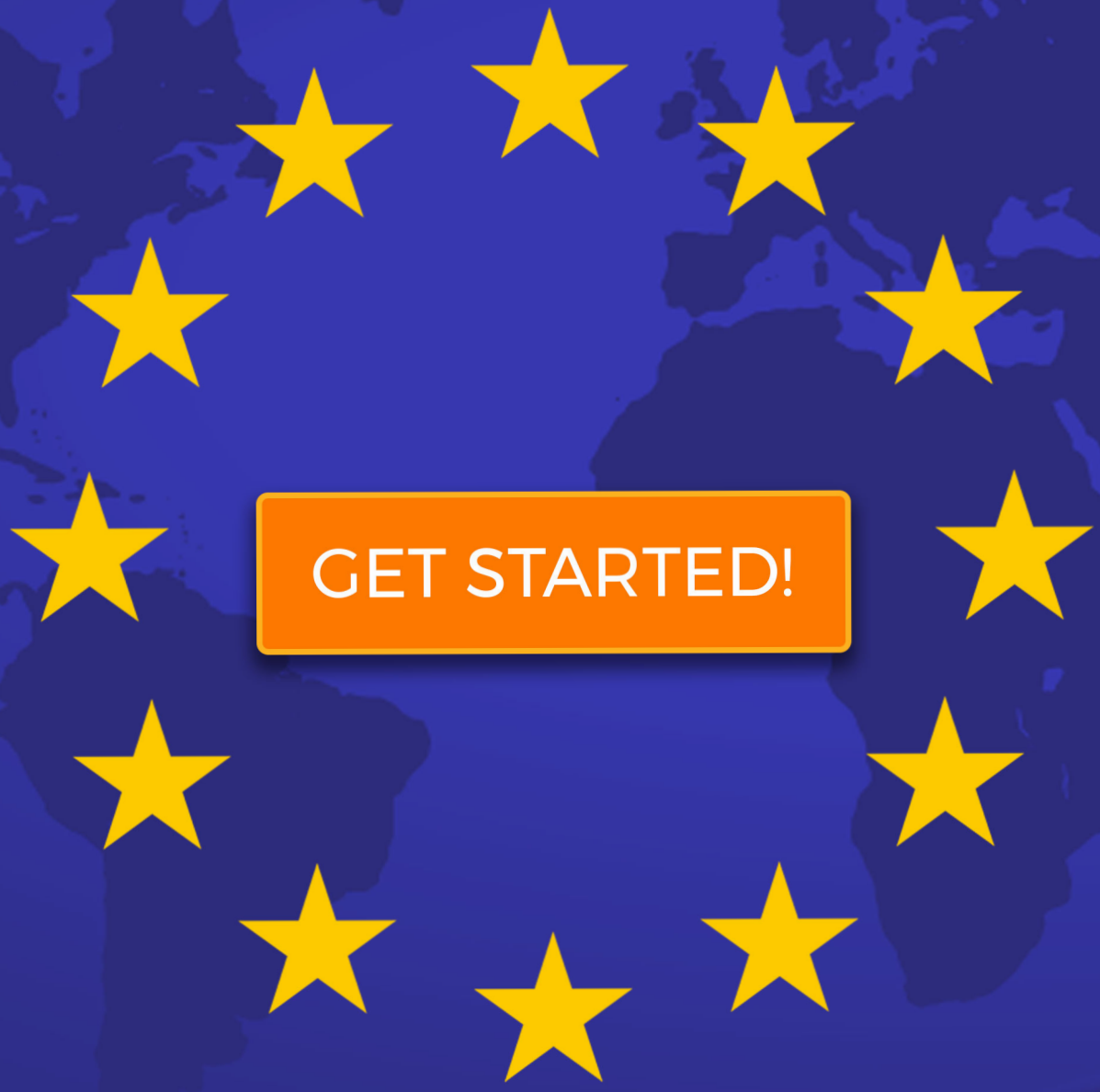
Natural Person
An individual human being, as distinguished from a private or public organization (see *Legal person*)

Personal Data
Any information relating to an identified or identifiable natural person

Processing
Any operation performed on personal data, whether or not by automated means

Processor
Natural or legal person, public authority, agency or other body which processes personal data on behalf of a controller

BE GDPR COMPLIANT WITH 360SUITE



GET STARTED!

360 Suite

Visit https://360suite.io