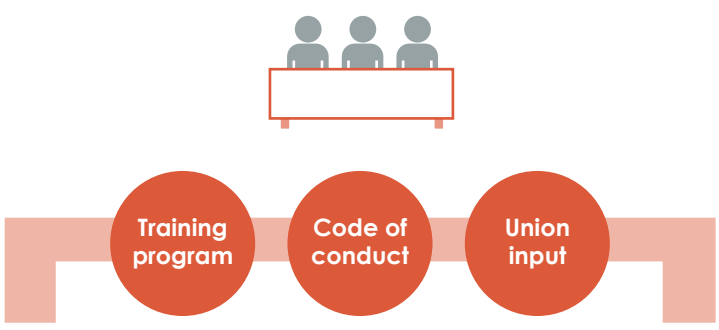
Kramer Levin

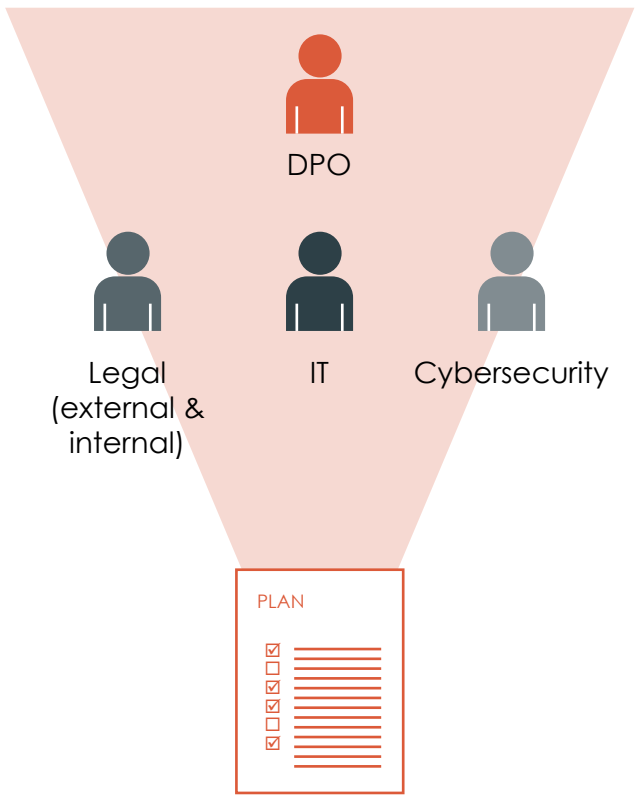
Getting on the right track for GDPR

In less than four months the EU's General Data Protection Regulation (GDPR) will go into full effect, bringing with it an array of new individual rights and regulatory requirements. It is not too late for organizations to join the race to ensure compliance. Here are some of the most important steps they should take to stay on the right track.



Set up a governance framework

Organizations will have to implement a **global data protection compliance program** and integrate it within the internal audit plan. They should set up an appropriate training plan, and may adhere to an approved code of conduct to demonstrate compliance. The board of directors should also be regularly informed (and involved, in the case of a serious data breach), and unions may be entitled to offer input on employee-related policies.



Designate a data protection officer (DPO)...

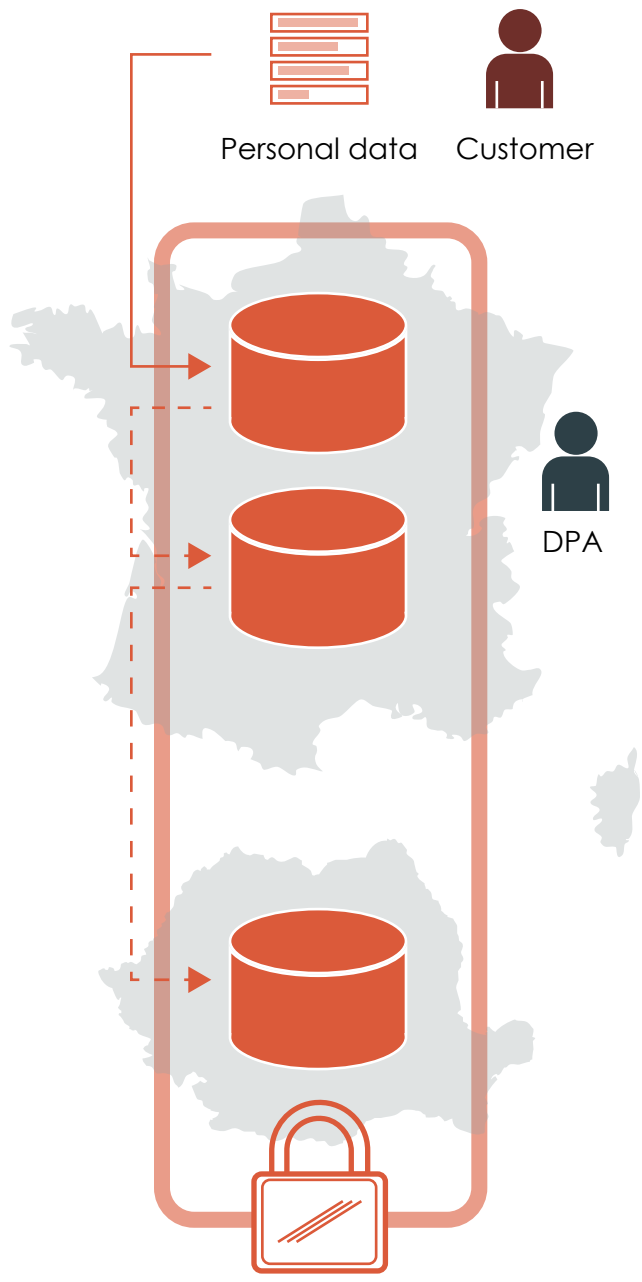
Organizations are highly encouraged to appoint a **DPO**, whose status has been reinforced. The DPO not only should be given sufficient autonomy and resources but also should report directly to the highest level of management.

...and a cross-disciplinary team

Considering the issues at stake and the need for robust governance, it is crucial for organizations to adopt a project-based approach led by a cross-disciplinary team composed of lawyers (internal and external) and cybersecurity and IT experts.

Develop a compliance plan

Organizations should define a plan to set up or assess their data compliance program, including an information audit of personal data and its processing, a risk assessment of such processing, implementation of GDPR-driven principles and policies, and continuous improvement and monitoring.



Know what data you hold and process

Organizations should ensure that they clearly understand and document what personal data they actually hold and what data is processed and transferred—including outside of the EU—and should control data flow within the organization.

Determine your lead DPA

Any organization that carries out **cross-border processing** and operates in several EU member states should determine its lead Data Protection Authority (DPA) and document the determination. Organizations should also verify whether other DPAs have competing jurisdiction.

Upgrade security and confidentiality

Organizations will have to rethink their data access management, tighten their access control and tracking, and review their confidentiality strategy. Data protection and privacy principles will also have to be integrated at the earliest stage of data processing design, including the adoption of robust internal policies and the principles of "**privacy by design and by default**."

For more information, contact Noëlle Lenoir nlenoir@kramerlevin.com or Alan R. Friedman afriedman@kramerlevin.com.