Company PROFILE

BARIZI
DATA
PROTECTION
SERVICES

www.bdps.co.ke

The Background (MISSION)

Barizi Data Privacy Services is a trusted, data protection service provider that allows you to outsource a range of much needed data protection and related services to ensure that your organization complies with the Data Protection Laws and Regulations, from across the globe.

Our mission is to help your organization keep up with global best practice in data protection and cyber security by offering a range of data protection and cyber security services.

Our practice combines experts from the ICT, Legal and Cyber Security practice areas to offer you a quality, comprehensive solution to all your Data Privacy, Cyber Security and Compliance needs.

1.0

Key Service offering for the website: -

1.1 VIRTUAL DATA PROTECTION OFFICER

(a) Full time DPO (Main service offering)

Our virtual Barizi DPO offers an effective solution for organizations that may require a DPO but do not wish to hire a full time in-house DPO.

Our goal is to provide you with a cost effective solution with the benefit of our years of experience, without having to worry about HR requirements.

This includes providing you with a named Data Protections Officer (DPO), supported by our wider team of specialists, to assist your organization in:

- Advisory-advising the data controller or data processor and their employees on data processing requirements provided under the Act or any other laws/regulations;
- Compliance-ensuring compliance with the Data Protection Laws and regulations;
- Capacity Building facilitating capacity building of staff involved in data processing operations;
- DPIA-providing advice on data protection impact assessment; and
- co-operating with the DPC and any other authority on matters relating to data protection.

(b) Part Time DPO

For organizations that may already have a full time DPO but require additional resource or on a need basis, we provide you with an interim who will serve as your independent data protection officer for the required period.

Our Interim DPO offers you all the services as required to by the Data Protection Act, within the period you require.

1.2 DATA PROTECTION ADVISORY

At Barizi Data Privacy Service, we do not just answer your concerns and questions we provide practical solutions tailored to the needs of your organization.

Barizi Data Privacy Service helps your organization to develop a bespoke solution, tailor made for your organization to help you maintain ongoing compliance with data privacy laws.

We recognize the special data compliance requirements vary from industry to industry and we provide you with consultancy service by our most experienced experts depending on the industry and organizational needs.

This includes Consultancy on:

1. Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) describes a process designed to identify risks arising out of the processing of personal data and to minimize these risks as far and as early as possible. DPIAs are important tools for negating risk, and for demonstrating compliance with the Data Protection Laws and global compliance standards

The DPA under Section 31 mandates that a DPIA shall be carried out where the processing of data shall result in a high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context, and purposes

At Barizi Data Privacy services, we conduct project based Data Protection Impact Assessments to enable you identify and mitigate against any data protection related risks arising from a new project, which may affect your organization or the individuals you engage with.

2. Data Subject Management

Data subjects are the individuals, whose personal data is processed by an organization. The Data Protection Act and the GDPR affords data subjects the right to access personal data and supplementary information, the right to have inaccurate personal data rectified, or completedif it is incomplete, the right to erasure in certain circumstances.

Data subjects may wish to enforce their rights to access, correct, or erase data held by the Organizations that hold personal data of consumers. With this in mind organizations need to be prepared for the management of these requests.

At Barizi Data Privacy Services we help you to manage and respond to data subject access request through our Data Subject Access Requests (SAR) and Data Subject Access Requests (SAR) quality assurance services

We review any redaction work, provide an assessment of your organizations completed documentation, and ensure compliance with relevant data protection laws.

We provide you with an evaluation of the documents, and provide expert advice on any amendments, deletion if necessary.

3. Ecommerce and ICT Consultancy

We advise you and guide you in the implementation of emerging and recurrent best practice Ecommerce and ICT standard and policy guide lines (including internet policies, terms of use of website and cookies policies).

4. Regulatory Representation

Barizi Data Privacy Services provides representation to our clients who have been the subject of regulatory subpoenas, inquiries and actions initiated by the Data Commissioner.

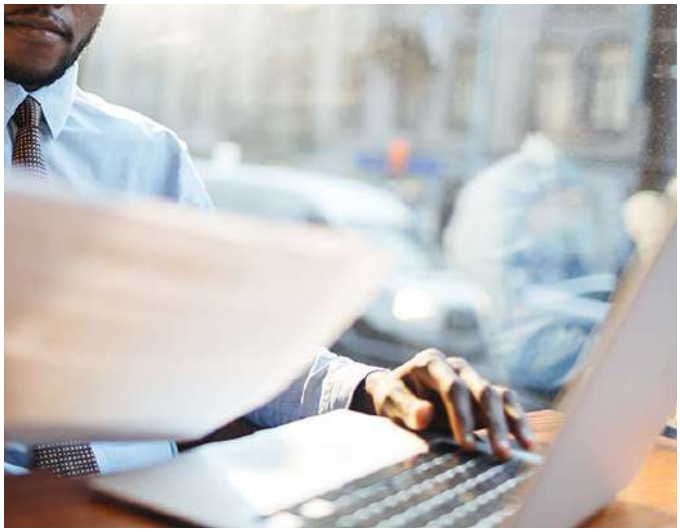
We act on your behalf to respond to inquiries, submit evidence or relevant documents subject to request from the Data Commissioner and general correspondence with the office of the Data Commissioner.

4. Data Protection Health Check

For organizations that are unsure as to whether they are compliant with the relevant Data Protection Laws generally, Barizi Data Privacy Service offers routine Data Protection Audits.

Work with our experts to thoroughly examine your data processing and storage systems and identify loop holes in your organizations data processing process and possible areas of liability exposure.

DPA 2019 CONSULTANCY



Our mission is to help businesses and organizations comply with the Data Protection Act (DPA) of 2019 in Kenya.

How can this service help you?

Our team of experts can help your organization comply with the DPA in the following ways:

1. Data Protection Impact Assessments (DPIA): We c help you conduct DPIAs to identify and assess the risks associated with your organization's data processing activities.

2. Data Protection Officer (DPO) services: We can provide you with a qualified and experienced virtual DPO to ensure that your organization complies with the DPA.

3. Data breach management: We can help you manage data breaches and ensure that you comply with the DPA's notification requirements.

4. Data protection training: We can provide your staff with training on data protection principles, best practices, and the DPA's requirements.

5. Data protection policies and procedures: We can help you develop and implement data protection policies and procedures that comply with the DPA.

Why choose Us?

At BDPS, we have a team of experts with extensive experience in data protection and privacy laws. We keep up to date with the latest developments in data protection and privacy laws in Kenya and globally. Our services are tailored to meet the specific needs of your organization, and we provide cost-effective solutions that are scalable to your organization's size and complexity.

GDPR CONSULTANCY

If you are a business operating in the European Union or dealing with EU citizens' personal data, you are subject to the General Data Protection Regulation (GDPR). This regulation is designed to protect the privacy of individuals and to give them control over their personal data.

At BDPS, we provide expert guidance on GDPR compliance, helping businesses to understand their obligations and implement necessary measures to ensure compliance. Our team of experienced consultants will work with you to assess your current practices and develop a customized GDPR compliance program tailored to your business needs.

Our consultation services include:

1. GDPR Compliance Assessment: We will conduct a comprehensive assessment of your current data protection practices to identify any gaps in compliance with GDPR.
2. Data Protection Officer (DPO) Services: We can provide a Data Protection Officer (DPO) to help ensure that your organization complies with GDPR requirements.
3. GDPR Training: We offer GDPR training sessions for your employees to help them understand their responsibilities and obligations under GDPR.
4. Data Protection Impact Assessment (DPIA): We can assist you in carrying out a DPIA to assess the risks associated with processing personal data and to identify measures to mitigate those risks.
5. GDPR Implementation: We can provide support in implementing GDPR requirements, including policy development, data mapping, and data protection impact assessments.
6. GDPR Auditing: We offer GDPR auditing services to help you ensure that your organization is fully compliant with GDPR.

This consultation service is designed to provide comprehensive and cost-effective support to businesses of all sizes. We understand that GDPR compliance can be complex and time-consuming, which is why we work closely with our clients to provide practical solutions that are easy to implement.

ISO/IEC 27701 CONSULTATION

ISO/IEC 27701 is a standard that provides guidelines for implementing and managing a privacy information management system (PIMS). The standard is based on the ISO/IEC 27001 information security management system (ISMS) standard and focuses on the protection of personally identifiable information (PII).

BDPS provides consultation services for organizations that want to implement ISO/IEC 27701. Our team of experts can guide you through the process of establishing and maintaining a PIMS that meets the requirements of the standard.

Here are some of the key areas where our consultation services can assist you:

1. Gap analysis: Our team can conduct a gap analysis to assess your current privacy management practices and identify areas where improvements are needed to meet the requirements of ISO/IEC 27701.

2. Risk assessment: We can help you identify and assess privacy-related risks that your organization faces, including those related to the collection, storage, use, and disclosure of PII.

3. Privacy policy development: We can assist you in developing a privacy policy that meets the requirements of ISO/IEC 27701 and is tailored to your organization's specific needs and requirements.

4. PIMS implementation: Our experts can guide you through the process of implementing a PIMS that meets the requirements of the standard. This includes defining roles and responsibilities, developing procedures, and establishing metrics to measure the effectiveness of your PIMS.
5. PIMS maintenance: We can help you ensure that your PIMS remains effective over time by conducting regular audits, reviewing policies and procedures, and updating your PIMS as needed.

6. Training and awareness: Our team can provide training and awareness sessions for your employees to help them understand the importance of privacy management and their role in maintaining an effective PIMS.

At BDPS, we understand the importance of protecting PII and the challenges that organizations face in implementing and maintaining an effective PIMS. Our consultation services can help you achieve compliance with ISO/IEC 27701 and build trust with your customers and stakeholders by demonstrating your commitment to privacy management.

1.3 Data Registration Services

At BDPS we advise you on the registration requirements, to help you determine whether you meet the thresh hold for mandatory registration as Data Controller or Data Processor, under the law s and regulations

We then guide you and undertake the registration process on your behalf including;

- → Identifying and describing various categories of personal data
- → Describing the purpose for which personal data is to be processed.
- → Categorization of Data Subjects
- → Guide and help in the filing of Application Forms
- → Follow up with the ODPC to acquire your registration certificate or renewal of certificate

1.4 International Data Transfer Compliance

The Data Protection Act requires, certain prior strict compliance requirements for Data Controllers and Data Processors before that are allowed to transfer and process Data outside the country.

We help you comply with this requirement by offering you the following services:

- **Liaison with the office of the Data Protection Commissioner**

We correspond with the office of the Data commissioner on your behalf to:

- Provide evidence of appropriate safeguards with respect to the security and protection of personal data, and the appropriate safeguards including jurisdictions with commensurate data protection laws;

- Demonstrate the effectiveness of the security safeguards or the existence of compelling legitimate interests, upon the request of the Data Commissioner.

- **Obtaining consent from the Data Subjects**

We assist you to obtaining consent of a data subject and on obtaining confirmation of appropriate safeguards.

- **Kenyan Data Center Representative**

For certain nature of processing that can only be effected through a server or a data centre located in Kenya, we offer our offices as data centers and provide you with the necessary establishment details such as an email address, local telephone number answered in the local language, physical address, and a translation service that enables us to correspond in any major language.

Our representation service also includes access to our advice line service and regular information and advice on data protection issues that may impact your operations.

1.5 Cyber Security Services.

The services offered under Cyber Security Services supplement your effort to ensure that your organisation effectively protects its data and is compliant with the best practice Global Data Protection regulations and set standard.

- **Cyber Security Consultancy**

Our team of cyber security consultants, will help you review and identify problems, evaluate security issues, assess risk, and implement solutions to defend against threats to companies' networks and computer systems.

We deal with many variables when evaluating security systems and craft layers of protection in a fast-changing IT landscape.

Our Cyber Security Consultancy includes a Cyber security review and a cloud security review, where our experts evaluate tests and analyzes an organization's cloud infrastructure to ensure the organization is protected from a variety of security risks and threats.

- Cyber Security Review- Our team will help your organization to identify the emerging or existing cyber threats to your organization and help you understand your level of cyber security exposure and identify areas.
- Cloud Security Review- A cloud security review involves an evaluation that tests and analyzes an organizations cloud infrastructure to ensure the organization is protected from a variety of security risks and threats.

- **ISO on Cyber Security Consultancy**

At BDPS, where we provide expert guidance on ISO cyber security standards to help your organization safeguard your digital assets and ensure compliance with regulatory requirements.

We understand that cyber security is a critical aspect of any organization's risk management strategy. With increasing cyber threats and the potential for data breaches, it's essential to have a robust cyber security framework in place. This is where our consultancy services can help.

Our team of experienced cyber security consultants will work with you to assess your organization's cyber security posture and develop a tailored solution based on your specific requirements. We specialize in ISO cyber security standards, including ISO/IEC 27001 and ISO/IEC 27002, and can help your organization achieve compliance with these

standards.

ISO/IEC 27001 is a widely recognized standard for information security management systems (ISMS). Our consultants can help you implement an effective ISMS framework that addresses the specific risks and threats faced by your organization. This includes identifying and assessing risks, implementing controls, monitoring and reviewing the system, and continually improving the effectiveness of the ISMS.

ISO/IEC 27002 provides a code of practice for information security management. Our consultants can help you implement the controls and best practices outlined in this standard to protect your organization's information assets.

We also offer consultancy services on other ISO cyber security standards, including ISO/IEC 27017 and ISO/IEC 27018, which provide guidance on cloud security and the protection of personal data, respectively.

Our consultancy services are tailored to your organization's needs, and we work closely with you to understand your business objectives and develop a cyber-security solution that aligns with your goals. We provide guidance and support throughout the implementation process and beyond, helping you maintain and continually improve your cyber security posture.

- **Security Posture Assessment**

Security posture assessments should be a continuous exercise to respond to an organization's growing cyber threats. Our security posture assessments framework includes a holistic analysis of the personnel, processes, policies and technologies of your organization to identify possible gaps in your security posture.

Our security posture assessment, assesses the controls and processes you have in place to protect your enterprise from cyber-attacks, your ability to detect and contain attacks, your ability to react to and recover from security events and the level of automation in your security programs.

- **Supply Chain Security Services**

Supply chain security largely entails avoiding risks associated with employing software built by another company and securing organizational data accessed by a third party in your supply chain.

We assist in protecting your assets from cyber threats through the use of security management systems that achieves a more secure, efficient flow of commodities that can quickly recover from interruptions.

Management of IT and Enterprise Architecture:

We will review IT management to verify the reliability and develop an organizational structure and procedures to ensure a controlled and efficient environment for information processing.

- **System Security Compliance**

We help your organisation to achieve Cybersecurity compliance by adhering to standards and regulatory requirements set forth by law and industry best practice regulations.

- **Information Processing Facilities:**

Our team will review to verify that the processing facility is controlled to ensure timely, accurate, and efficient processing of applications under normal and potentially disruptive conditions.

- **Penetration Testing**

We assist in conducting Ethical hacking into the system. This entails the intentional launching of simulated cyberattacks that seek out exploitable vulnerabilities in your computer systems, networks, websites, and applications. Through the process, we seek to provide you with the deep solution to fix the vulnerabilities identified within your system.

- **Cybersecurity Incident and Post Breach Incident Management**

In the event your company or organization suffers a security breach, we are here to help provide a fast and effective response. Time is always of the essence, so our team offers immediate pragmatic solutions, as well as general advice on how best to technically respond to a breach scenario.

- **Cybercrime, Cybersecurity and Data Breaches Litigation Support**

Have you suffered a cybercrime incident? Work with our team of cyber security expert investigators to effectively prosecute the crime and seek appropriate civil remedies. We partner with you or your company immediately following a cybercrime incident (such as email and internet fraud, identity fraud, theft and sale of corporate data, cyber extortion, online slander/defamation etc) to offer Cybercrime and Data Breaches Litigation support, which includes:

- Reporting to the relevant authorities
- Gathering material evidence to support the prosecution of the crime or civil litigation
- Providing you with our expert witness to testify in court

1.6 Data Backup Services

We help you create copies of important data and files on secure remote servers, so that they can be accessed and restored in case of data loss or disaster. We offer cloud backup services that are compliant with industry-specific regulations and data protection laws, helping organizations to meet their legal and regulatory obligations.

1.7 TRAININGS

We offer training on how to comply with the Data Protection laws both locally and internationally. This includes understanding the principles of data protection, identifying data subjects' rights, and how to handle data breaches.

Learn about :

Data Privacy Impact Assessment (DPIA) - Our courses teach you how to conduct DPIAs effectively. This is a critical aspect of GDPR compliance as it helps identify and minimize risks to data subjects' rights and freedoms.

Data Protection by Design and Default - We provide training on how to implement data protection by design and default principles into your business processes. This is crucial as it ensures that data protection is considered at every stage of the development process.

Cybersecurity - Our courses cover cyber security practices that can help you protect sensitive data from malicious attacks. This includes implementing access controls, encrypting data, and training employees on how to recognize and respond to cybersecurity threats.

Records Management - We provide training on how to manage records effectively. This includes understanding retention periods, securely destroying data, and ensuring that records are accurate and up-to-date.

Our training courses are designed for individuals or businesses of all sizes, from small start-ups to large corporations. We offer both on-site and remote training options, and our trainers are experienced professionals in the field of data protection. Our courses are tailored to meet the specific needs of each client, ensuring that you receive training that is relevant to your business.

We understand that data protection is an ever-evolving field, and we strive to keep our training courses up-to-date with the latest developments. Our courses are regularly reviewed and updated to ensure that you receive training that reflects the most current data protection regulations and best practices.

FAQ's

1. Who is a virtual Data Protection Officer (DPO)

1. WHO IS A VIRTUAL DATA PROTECTION OFFICER (DPO)

A virtual Data Protection Officer (DPO) is a professional who provides data protection and privacy services to businesses remotely, typically on a part-time or as-needed basis. They are responsible for ensuring that a company's data protection practices comply with applicable laws and regulations,.

2. CAN A VIRTUAL DPO PROVIDE THE SAME LEVEL OF SUPPORT AS AN IN-HOUSE DPO?

Yes, a virtual Data Protection Officer (DPO) can provide the same level of support as an in-house DPO, provided they have the necessary qualifications, experience, and expertise to fulfill the role.

A DPO is responsible for advising and guiding their organization on compliance with data protection regulations, monitoring the organization's data protection practices, and acting as a point of contact for data protection authorities and data subjects.

Whether an in-house or virtual DPO, they must have the required knowledge, skills, and expertise to perform these tasks. An organization should select a DPO who has expertise in data protection law and practices, and who understands the specific risks and challenges faced by their organization.

3. WHAT ARE THE BENEFITS OF HIRING A VIRTUAL DPO VERSUS AN IN-HOUSE DPO?

A Data Protection Officer (DPO) is a critical role in ensuring that an organization complies with data protection regulations. When it comes to hiring a DPO, organizations have two options: hiring an in-house DPO or a virtual DPO. Here are some benefits of hiring a virtual DPO over an in-house DPO:

1. Cost-effective: Hiring a virtual DPO is often more cost-effective than hiring an in-house DPO. With a virtual DPO, you only pay for the services you need, whereas an in-house DPO requires a full-time salary, benefits, and other expenses.

2. Expertise: Virtual DPOs often have more extensive expertise in data protection and privacy regulations because they work with multiple clients across different industries. This means they can provide a broader range of insights and guidance to your organization.

3. Flexibility: A virtual DPO can work with your organization on a flexible schedule and as needed, rather than requiring a full-time presence in your office.

5. Reduced Conflict of Interest: An in-house DPO may face conflicts of interest when required to report to company management while at the same time ensuring compliance with data protection regulations. With a virtual DPO, there is less potential for such conflicts.

6. Access to a Wider Talent Pool: With a virtual DPO, you have access to a wider pool of talent across the world, allowing you to find the right person with the specific skills and experience your organization needs.

It is important to note that whether you choose an in-house DPO or a virtual DPO, the DPO must have the necessary knowledge and skills to carry out their duties effectively.

4. WHAT ARE SOME OF THE WAYS A VIRTUAL DPO CAN HELP YOUR BUSINESS?

Overall, a virtual DPO can help your business develop and implement effective data protection strategies, ensure compliance with relevant laws and regulations, and protect your business from potential data breaches and other data protection risks by:

1. Ensuring compliance with data protection laws: A virtual DPO can help your business stay compliant with the various data protection laws and regulations that apply to your organization. They can provide guidance on best practices, conduct audits, and help you develop and implement policies and procedures to protect personal data.

2. Managing data breaches: A virtual DPO can help your business respond to data breaches by providing guidance on how to investigate and contain the breach, notifying affected individuals, and reporting the breach to relevant authorities as required by law.

3. Conducting risk assessments: A virtual DPO can conduct risk assessments to identify potential data protection risks and help your business mitigate them. This includes assessing the security of your data systems, identifying vulnerabilities, and developing strategies to address them.

4. Training employees: A virtual DPO can provide training to your employees on data protection best practices, policies, and procedures. This can help your employees understand the importance of data protection and how to comply with relevant laws and regulations.

5. Serving as a point of contact: A virtual DPO can serve as a point of contact for data protection authorities, customers, and other stakeholders. They can help your business respond to data protection inquiries and requests, and communicate with stakeholders about your data protection practices.

5. HOW DO I KNOW IF MY BUSINESS NEEDS A VIRTUAL DPO?

A virtual Data Protection Officer (DPO) is a professional who provides data protection advice and guidance to businesses without being physically present in the company. If you're unsure whether your business needs a virtual DPO, here are a few things to consider:

1. Does your business process large amounts of personal data? If your business processes a significant amount of personal data, it may be beneficial to have a virtual DPO to ensure compliance with data protection laws.

2. Is your business in a highly regulated industry? If your business operates in a highly regulated industry, such as healthcare or finance, a virtual DPO can help ensure compliance with complex data protection regulations.

3. Does your business lack in-house expertise in data protection? If your business does not

have staff with expertise in data protection, a virtual DPO can provide the necessary guidance and support.

4. Do you want to reduce costs associated with hiring a full-time DPO? If your business is small or medium-sized and does not have the resources to hire a full-time DPO, a virtual DPO may be a more cost-effective solution.

Ultimately, the decision to hire a virtual DPO depends on your business's specific needs and circumstances. It may be helpful to consult with a data protection expert to determine whether a virtual DPO is the right choice for your business.

6. WHAT QUALIFICATIONS AND EXPERIENCE SHOULD A VIRTUAL DPO HAVE?

1. Expertise in data protection regulations: A virtual DPO should have in-depth knowledge and understanding of data protection laws, such as the Data Protection Act (DPA,2019) EU General Data Protection Regulation (GDPR) , or other relevant regulations.

2. Experience in data protection: A virtual DPO should have relevant experience in data protection, preferably in a similar role.

3. Qualifications: While not a strict requirement, a virtual DPO should ideally hold relevant qualifications in data protection, such as the Certified Information Privacy Professional (CIPP) or Certified Information Privacy Manager (CIPM) certifications.

4. Legal background: A virtual DPO with a legal background can be particularly valuable in providing legal advice on data protection matters.

5. Industry-specific knowledge: A virtual DPO with experience in your industry can provide valuable insights into sector-specific data protection risks and compliance requirements.

7. HOW LONG DOES IT TAKE TO SET UP A VIRTUAL DPO SERVICE?

The setup time for a Virtual Data Protection Officer (DPO) service can vary depending on several factors, such as the complexity of your organization's data processing activities and the level of customization required for the service.

However, typically, the setup process for a Virtual DPO service can take anywhere from a few days to a few weeks

8. HOW DOES A VIRTUAL DPO ENSURE COMPLIANCE WITH DATA PROTECTION REGULATIONS?

A Data Protection Officer (DPO) is a key position within an organization responsible for ensuring compliance with data protection regulations). In the case of a virtual DPO, their role and responsibilities remain the same, but they perform their duties remotely.

Here are some ways a virtual DPO can ensure compliance with data protection regulations:

1. Develop and implement policies and procedures: The DPO can develop and implement data protection policies and procedures that are in line with the relevant data protection regulations. These policies can cover data collection, processing, storage, and deletion.

2. Conduct audits and risk assessments: The DPO can conduct regular audits and risk assessments to identify and mitigate potential data protection risks. This can involve reviewing data protection policies and procedures, as well as assessing the security measures in place for protecting data.

3. Provide training and awareness: The DPO can provide training and awareness sessions to employees on data protection regulations and best practices. This can help employees understand their roles and responsibilities in protecting personal data and ensure compliance with regulations.

4. Monitor compliance: The DPO can monitor compliance with data protection regulations by reviewing data protection policies, assessing data protection risks, and conducting regular audits. They can also ensure that any breaches of data protection regulations are reported to the relevant authorities as required.

5. Stay up to date with data protection regulations: The DPO can stay up to date with changes in data protection regulations and best practices by attending relevant training, conferences, and webinars. This can help them keep abreast of any changes that may impact the organization's data protection policies and procedures.

Overall, a virtual DPO can play a crucial role in ensuring that an organization remains compliant with data protection regulations, despite the physical distance from the organization.

9. WHAT ARE THE KEY RESPONSIBILITIES OF A VIRTUAL DPO?

A Data Protection Officer (DPO) is responsible for ensuring that an organization's processing of personal data complies with applicable data protection laws and regulations. In the context of a virtual DPO, the responsibilities are similar, but the DPO performs their duties remotely. Here are some key responsibilities of a virtual DPO:

1. Advising the organization: The virtual DPO advises the organization on its obligations under data protection laws and regulations, and provides guidance on how to comply with those obligations.

2. Monitoring compliance: The virtual DPO monitors the organization's compliance with data protection laws and regulationsand other applicable laws.

3. Managing data protection risks: The virtual DPO identifies and assesses data protection risks associated with the organization's processing of personal data, and develops and implements measures to mitigate those risks.

4. Conducting audits and assessments: The virtual DPO conducts regular audits and assessments of the organization's data protection practices to ensure compliance with applicable laws and regulations.

5. Managing data subject requests: The virtual DPO manages data subject requests, including requests for access, rectification, erasure, and portability of personal data.

6. Training staff: The virtual DPO provides training and guidance to staff on data protection laws and regulations, as well as the organization's data protection policies and procedures.

7. Liaising with authorities: The virtual DPO serves as the primary point of contact for data protection authorities, and communicates with them as needed regarding the organization's data protection practices.

10. CAN A VIRTUAL DPO BE HELD PERSONALLY LIABLE FOR ANY BREACHES OR NON-COMPLIANCE ISSUES WITHIN AN ORGANIZATION?

The liability of a virtual DPO may depend on the terms of their contract and the level of control they have over the organization's data protection practices. If the virtual DPO has limited access to the organization's systems and data, and their role is advisory in nature, their liability may be limited. However, if the virtual DPO is responsible for overseeing the organization's data protection practices and has the authority to make decisions and enforce compliance, their liability may be higher.

11. IS IT MANDATORY FOR A BUSINESS TO REGISTER AS A DATA CONTROLLER OR DATA PROCESSOR?

It is not mandatory to register ,however, where

data is processed for the following listed purposes, it is mandatory for the Data Controller and Data Processor to comply with registration requirement:

1. Canvassing political support among the electorate.

2. Crime prevention and prosecution of offenders (including operating security CCTV system).

3. Gambling.

4. Operating an educational institution.

5. Health administration and provision of patient care.

6. Hospitality industry firms but excludes tour guides.

7. Property management including the selling of land.

8. Provision of financial services.

9. Telecommunication networks or service providers

10. Transport service firms

11. Businesses Processing genetic data

12. Businesses wholly and mainly in direct marketing

Stay a Step Ahead of Cyber Security Threats

BARIZI
DATA
PROTECTION
SERVICES

GET IN TOUCH

+254 112 774 227

info@bdps.co.ke

Location :

I&M Bank House, 5th Floor,
2nd Ngong Avenue, Upper Hill,
Nairobi, Kenya