EY DPO as a Service

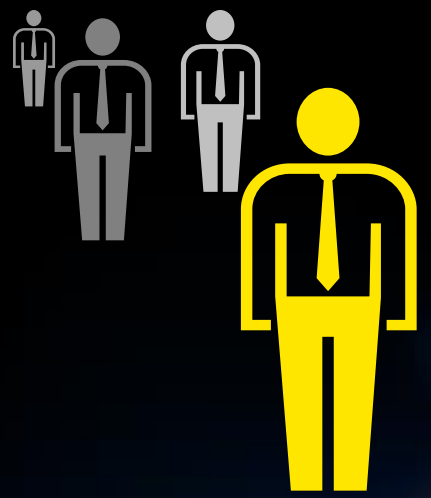
EY Ukraine Digital

The better the question. The better the answer. The better the world works.

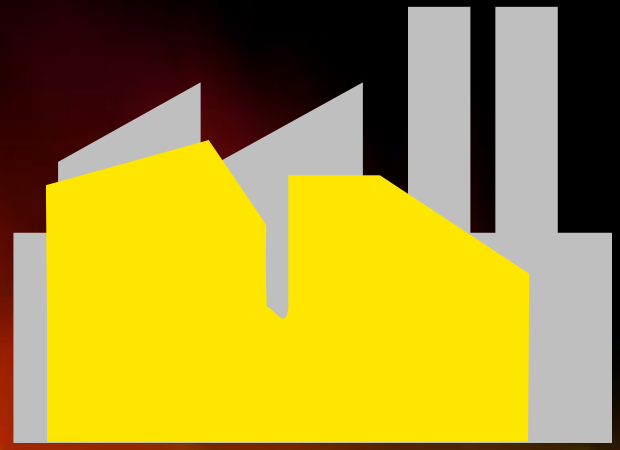
Shape the future with confidence

Do you have a Data Protection Officer, who provides privacy leadership in your organization?

We propose a solution - DPO as a Service – your one-stop-shop in privacy leadership



Your dedicated DPO from us,
and team of experts behind



Being a part of your organization
to improve privacy posture

Analyze

Conduct a detailed analysis of data processing by documenting personal data sources and purposes, creating an inventory of processing activities, evaluating data collection protocols, and assessing risks to personal data.

Govern

Implement a governance framework that promotes accountability for data protection, includes regular compliance audits, and provides comprehensive training for employees

Manage

Implement a holistic approach to data protection by establishing clear consent processes and ensuring compliance with the privacy laws and regulatory requirements for data collection and cross-border transfers.

Integrate

Implement and operate a robust data protection framework that features an incident response plan for breaches, standardized contracts with data protection clauses, and a centralized registry of third-party relationships

How is your organization managing data privacy?

Market trends

Over the last few years, companies in every industry around the globe have seen their sensitive internal data or personally identifiable information lost, stolen or leaked to the outside world. A wide range of high-profile data loss incidents have cost organizations millions of dollars in direct and indirect costs and have resulted in tremendous damage to brands and reputations.

The rising costs and increased media coverage of data breaches and the continuous evolution of threats facing organizations means this is being discussed at the highest level of our clients.

12% of respondents say that their organization has experienced a material privacy breach over the past 12 months.*

Nine in ten medium and large companies already have Privacy Offices – a figure unchanged from last year. But among companies under $50M, adoption surged from 31% in 2024 to 87% in 2025. **

Source:
1.: STATE OF PRIVACY 2025, ISACA
*2.**Trustarc 2025 Global Privacy Benchmarks report*

Organizations continue to be plagued by sensitive data or personal data protection challenges

Compliance

Organizations want to better navigate and ensure compliance to applicable data privacy laws and regulatory requirements (e.g., GDPR, HIPAA, PCI DSS), to minimize the risk of financial, compliance, and reputational impacts to their organization.

Use of personal data

Organizations want to better anticipate and manage the challenges around adopting cloud technology, especially when a hybrid environment (on-premise and cloud applications) is required.

An important aspect the way new implemented technologies process personal data and how they conduct to regulatory requirements.

Cost Efficiency

Rising costs for data protection are common challenge for Organizations, it is challenging to balance between technical solutions for data protection and their costs.

Organizations need to effectively manage the cost and complexity of managing privacy programs.

"Privacy by design"

Organizations need to implement privacy requirements when developing applications, new products or services.

On other hand, implementation of "Privacy by design" principle can make data privacy enabled by default.

The question is how to do it effectively and efficiently.

In today's fast-paced digital landscape, effective data and privacy protection and compliance to data privacy laws and regulatory requirements are critical for minimizing privacy risks and ensuring adherence to regulatory requirements. As privacy regulations evolve and data breaches become more frequent, organizations are facing growing exposure to legal and reputational risks, emphasizing the urgent need for strong compliance leadership to navigate these challenges.

DPO as a Service key qualifying questions

Are your existing capabilities allowing you to effectively manage privacy data and meet compliance?

1. How to effectively classify and manage personal data?
2. How to determine where to store, process, and transfer personal data between systems and third parties?
3. How to develop data protection policies and keep them up-to-date and in line with changes in regulatory requirements?
4. How to integrate personal data protection into business processes and the development of new services and products?
5. How to inform employees about personal data protection and their compliance obligations?

DPO as a Service – dedicated privacy and compliance leader

Service Overview

- DPO as a Service is a subscription-based data privacy and compliance leadership solution that provides organizations with on-demand support from dedicated experienced EY privacy manager and team of experts behind, providing tailored Privacy Implementation and compliance strategies
- This service enables businesses to effectively manage risks associated with sensitive data, comply with regulatory requirements, and adapt to evolving threats without the financial burden of hiring a full-time DPO
- By leveraging EY's expertise and resources, you gain a comprehensive privacy posture that aligns with their specific needs and GDPR standards

Key Features

- **On-Demand Expertise:** Access to your trusted EY privacy manager and team of professionals when you need them
- **Customized Strategy:** Development of tailored privacy plans that align with your business goals and industry requirements
- **Continuous Monitoring:** Ongoing assessment and reporting of your privacy posture to identify and mitigate risks
- **Regulatory Compliance Support:** Guidance on meeting industry regulations and standards to protect your organization
- **Incident Response Planning:** Preparation and support for responding to privacy incidents swiftly and effectively

Benefits

- **Cost-Effective:** Avoid the high costs associated with hiring a full-time DPO while still receiving expert guidance and legal support from professionals
- **Scalable Solutions:** Easily adjust the level of service based on client's changing needs
- **Enhanced Compliance:** Improve your organization's overall compliance to data privacy laws and regulatory requirements
- **Peace of Mind:** Focus on your core business while knowing that privacy and compliance is in expert hands

Approach

1 Analyze

- Conduct data mapping, inventory, and maintain the Record of Processing Activities for GDPR compliance
- Ensure appropriate data collection and classification to gather only relevant personal data
- Perform privacy impact assessments to identify risks and evaluate controls

2 Govern

- Establish accountability and compliance measures to uphold personal data protection standards
- Conduct internal and external assurance activities to evaluate personal data protection practices
- Provide training and awareness programs to educate staff on personal data protection responsibilities

3 Manage

- Implement privacy and security by design principles in all projects and processes
- Manage data subject rights effectively to ensure compliance with GDPR
- Define and document the use of data to align with legal requirements
- Establish clear consent mechanisms and privacy notifications for data subjects
- Ensure compliance with regulations regarding cross-border data transfers

4 Integrate

- Implement and operate incident and breach management procedures to address data privacy incidents effectively
- Establish records management practices to ensure proper handling and retention of personal data
- Manage third-party risks to ensure compliance with personal data protection requirements
- Enhance data protection and security measures to safeguard personal data

Key Success Metrics

- **Compliance Rate:** Percentage of compliance with relevant data protection regulations and GDPR standards
- **Strategy Completion:** Percentage of implemented privacy measures and initiatives within the planned timeline
- **Privacy Posture Improvement:** Reduction rate of identified privacy risks and compliance gaps over time

Service Dependencies

- **Client Collaboration:** Successful implementation relies on active participation and communication from the client's team
- **Resource Allocation:** Availability of budget and people resources from the client to support the implementation of recommended measures
- **Data Access:** The availability of relevant data and logs from the client's systems enables compliance with data processing activities

Key service delivery options

Basic – up to 20 hours/month

- **Access to a DPO:** On-demand access to your trusted experienced EY privacy manager and his team for ongoing support
- **Strategic Planning:** Development of a customized privacy strategy aligned with your privacy objectives
- **Operations guidance:** Provision of guidance on privacy operations and templates for privacy policies
- **Compliance Guidance:** Assistance in understanding and meeting relevant regulatory requirements (e.g., GDPR, HIPAA, CCPA)
- **Quarterly Review Meetings:** Regular check-ins to assess progress and adjust strategy as needed

Ideal For: Small to medium-sized enterprises (SMEs) looking for basic privacy leadership and compliance support.

Standard – up to 40 hours/month

- **All Basic Option Features:** Includes everything in the Basic Option
- **Continuous Monitoring:** Ongoing reviews of your environment to detect control inefficiencies
- **Incident Response Planning:** Development of a tailored incident response plan to ensure swift action during privacy incidents
- **Employee Training Monitoring:** Create and review regular training schedule for staff on privacy awareness
- **Monthly Security Reports:** Detailed reports on privacy posture, incidents, and compliance status delivered monthly

Ideal For: Organizations that require proactive monitoring and structured incident response capabilities.

Advanced – 80+ hours/month

- **All Standard Option Features:** Includes everything in the Standard Option
- **Operations execution:** Ongoing privacy processes execution
- **Crisis Management Support:** Real-time assistance during significant privacy incidents, including communication strategies and stakeholder management
- **Annual Privacy Review:** Comprehensive review of your privacy practices and compliance, with actionable recommendations for improvement

Ideal For: Enterprises or organizations with high-security needs that require robust, ongoing privacy leadership and support.

Chapter 2

Internal information about service

Detailed service approach

1 Analyze

- Conduct interviews with key personnel to understand data flows, storage locations, and processing activities
- Identify and document all personal data processed, including its sources, purposes, and retention periods.
- Create a comprehensive inventory of all data processing activities, including details on data types, processing purposes, and data subjects.
- Develop a detailed Record of Processing Activities that includes information on data controllers, processors, and the legal basis for processing.
- Evaluate the protocols for collecting personal data to ensure that the data is relevant, and that processing is limited to that necessary to achieve the purpose.
- Identify potential risks to personal data and evaluate the effectiveness of existing controls to mitigate those risks.

2 Govern

- Establish a governance framework to ensure accountability for data protection across the organization, assigning clear roles and responsibilities.
- Conduct regular audits and assessments to evaluate compliance with GDPR requirements and identify areas for improvement.
- Establish a mechanism for reporting and addressing compliance issues, ensuring that corrective actions are taken promptly.
- Develop and deliver comprehensive training programs for employees on privacy laws and regulatory requirements (e.g., GDPR, HIPAA, CCPA), data protection policies, and their responsibilities in safeguarding personal data.
- Evaluate the effectiveness of training programs through assessments and feedback, adjusting as necessary to enhance understanding and compliance.

3 Manage

- Integrate privacy and security measures into the design and development of new products and services from the outset.
- Establish clear processes for managing data subject rights, including access, rectification, erasure, and data portability requests.
- Implement a tracking system to monitor and respond to data subject requests in a timely manner, ensuring compliance with GDPR timelines.
- Define and document the purposes for which personal data is collected and processed, ensuring they align with GDPR principles.
- Implement data minimization strategies to limit the collection and retention of personal data to what is necessary for the intended use.
- Develop clear and transparent consent mechanisms that allow data subjects to provide informed consent for data processing activities.
- Create comprehensive privacy notices that inform data subjects about their rights, the purposes of data processing, and how their data will be used.
- Assess and document any cross-border data transfers to ensure compliance with GDPR regulations regarding international data transfers.
- Implement appropriate safeguards, such as Standard Contractual Clauses or Binding Corporate Rules, to protect personal data during cross-border transfers.

4 Integrate

- Establish a robust incident response plan to promptly identify, assess, and respond to data breaches and security incidents.
- Implement and operate a reporting mechanism for data breaches that complies with GDPR notification requirements, ensuring timely communication with relevant authorities and affected individuals.
- Develop a comprehensive records management policy that outlines procedures for the creation, retention, and disposal of personal data records.
- Implement and operate a systematic approach to categorize and archive records, ensuring easy retrieval and compliance with data retention policies.
- Develop standardized contract templates that include data protection clauses, ensuring that all agreements with third parties clearly outline their responsibilities and obligations regarding personal data handling.
- Maintain a centralized registry of all third-party relationships, documenting key information such as data processing activities, compliance status, and contract details.
- Develop a data protection policy that outlines the organization's commitment to safeguarding personal data and compliance with GDPR.
- Create standardized data protection clauses for inclusion in contracts with data processors and third parties to ensure compliance with GDPR requirements.

Business model lean canvas

Problem

Many organizations lack the expertise to manage privacy risks effectively

Small to medium-sized enterprises (SMEs) cannot afford a full-time Data Protection Officer (DPO)

Challenges in personal data protection require constant monitoring and adaptation of the strategy

Existing Alternatives

In-House DPO

DPO-as-a-service

Data privacy consulting

Trained employee with functions of DPO (without formal position)

Solution

On-demand access to experienced privacy professionals

Customized privacy strategy development and implementation

Continuous monitoring and reporting on privacy posture and compliance

Key Metrics

Compliance with privacy laws and regulations

Reducing risks of financial, compliance, and reputational impacts

Realization of the business strategy

Passed all privacy-related audit checkpoints

Unique Value Proposition

EY offers expert privacy leadership and operational support tailored to the specific needs of organizations, ensuring robust protection against evolving threats and requirements without the overhead of a full-time DPO

High Level Concept

Virtual DPO for everyone

On-demand privacy expertise

Easy privacy help when you need it

Legal support from professionals

Unfair Advantage

EY's established reputation and trust in the industry

Access to a vast network of privacy experts and resources

Comprehensive understanding of regulatory requirements and compliance standards

Channels

Direct sales through EY's existing client relationships

Digital marketing campaigns targeting SMEs and larger enterprises

Partnerships with technology providers and industry associations

Customer Segments

Small to medium-sized enterprises (SMEs) across various industries

Large enterprises looking for supplementary privacy leadership

Regulated Industries - businesses in sectors like finance, healthcare, and energy

Local businesses aiming to expand into European markets while ensuring compliance with data protection regulations

Early Adopters

Existing clients without privacy function

Startups in Tech and Fintech

Cost Structure

Salaries and benefits for EY privacy professionals

Marketing and sales expenses

Technology and tools for monitoring and reporting

Training and development for staff (e.g. certifications)

Revenue Streams

Subscription-based pricing model for ongoing DPO services

One-time fees for specific projects or assessments

Consulting fees for additional cybersecurity services (e.g., trainings, HIPAA compliance)

Client portrait (Small to Medium-Sized Enterprises)

Job titles

- Business Owners
- IT Managers
- Operations Managers
- Compliance Officers
- Chief Financial Officers (CFOs)
- Marketing Managers
- Human Resources Managers

Demographics

- Age: 30-55 years old
- Location: Major cities such as Kyiv, Lviv, Odesa, and Dnipro, as well as regional centers
- Education: Bachelor's degree or higher, often in business, IT, or related fields
- Income Level: From UAH 50,000 to UAH 200,000 monthly

Interests

- Privacy and Regulatory Compliance
- Business Development and Growth Strategies
- Risk Management and Compliance
- Technology Solutions and Innovations
- Networking with other business owners and professionals
- Community Involvement and Local Business Events
- Online Learning and Professional Development
- Digital Marketing and Social Media Strategies
- Financial Management and Cost Reduction Techniques

Pain Points

- Limited budget for privacy resources
- Lack of in-house expertise to manage privacy risks effectively
- Difficulty in keeping up with regulatory compliance requirements, especially with recent changes
- Concerns about the potential impact of privacy incidents on business operations and reputation
- Time constraints in managing cybersecurity alongside other business responsibilities
- Fear of losing customer trust due to data breaches
- Difficulty in understanding complex privacy jargon and solutions
- Challenges in training employees that work with personal on privacy awareness

Behavior

- Actively seeking information on privacy solutions and best practices
- Engaging with content related to business growth, technology, and risk management
- Participating in local business networks and online forums
- Likely to attend workshops and seminars on privacy and business management
- Regularly use social media platforms (e.g., Facebook, LinkedIn) for business networking and information sharing
- Tend to follow industry influencers and thought leaders on social media
- Participate in online courses or webinars to enhance knowledge
- Read industry publications and blogs to stay informed about trends

Client portrait (Enterprises with high-security needs)

Job titles

- Chief Information Security Officers (CISOs)
- IT Directors
- Compliance Managers
- Risk Management Executives
- Chief Technology Officers (CTOs)
- Security Analysts

Demographics

- Age: 35-60 years old
- Location: Major cities with significant corporate presence
- Education: Master's degrees in IT, Cybersecurity, Business Administration, or related fields
- Income Level: From UAH 50,000 to UAH 200,000 monthly

Interests

- Advanced Privacy Solutions and Technologies
- Regulatory Compliance and Risk Management
- Industry Trends and Best Practices in Privacy
- Networking with other executives and industry leaders
- Participation in privacy conferences and seminars
- Researching emerging technologies and innovations in privacy
- Leadership Development and Executive Coaching
- Strategic Planning and Business Continuity
- Data Analytics and Business Intelligence

Pain Points

- Complex organizational structures leading to fragmented privacy practices
- High stakes for compliance with industry regulations and potential penalties
- Need for supplementary privacy leadership to support existing teams
- Pressure to stay ahead of evolving privacy threats and vulnerabilities
- Resource allocation challenges in maintaining comprehensive security measures
- Difficulty in integrating new privacy technologies with existing systems
- Concerns about the effectiveness of current privacy measures
- Challenges in communicating privacy needs to upper management

Behavior

- Regularly conducting privacy assessments and audits
- Engaging with thought leadership content and industry reports
- Attending executive-level networking events and conferences
- Collaborating with cross-functional teams to enhance security posture
- Utilizing professional networking platforms (e.g., LinkedIn) for industry insights
- Participating in roundtable discussions and think tanks on privacy
- Following industry-specific news and updates to stay informed
- Engaging in continuous professional development through certifications and training

Client portrait (Digital Transformation Organizations)

Job titles

- Digital Transformation Officers
- IT Project Managers
- Chief Technology Officers
- Innovation Managers
- Business Analysts
- Change Management Specialists
- Data Analysts

Demographics

- Age: 30-50 years old
- Location: Regions with a strong focus on technology and innovation (e.g., Kyiv, Lviv, Odesa)
- Education: Bachelor's or Master's degree in IT, Business, or related fields; many have certifications in project management or digital transformation.
- Income Level: From UAH 40,000 to UAH 150,000 monthly

Interests

- Digital Transformation and Innovation Strategies
- Cloud Computing and SaaS Solutions
- Privacy Best Practices
- Agile Project Management
- Networking with technology and innovation professionals
- Continuous Learning and Professional Development
- User Experience (UX) and Customer Journey Mapping
- Data Privacy and Compliance
- Emerging Technologies (AI, IoT, Blockchain)

Pain Points

- Increased exposure to privacy threats during the transition to digital platforms
- Need for updated privacy strategies to protect new digital assets
- Balancing the speed of innovation with the need for privacy and compliance
- Concerns about the impact of privacy breaches on digital initiatives and customer trust
- Resistance to change within the organization regarding new technologies
- Difficulty in aligning privacy and business objectives during transformation
- Challenges in managing stakeholder expectations and communication
- Limited resources for implementing comprehensive privacy measures

Behavior

- Actively seeking expert guidance on integrating privacy into digital transformation initiatives
- Engaging with content related to digital innovation and privacy
- Participating in workshops and webinars focused on technology trends
- Utilizing online platforms for collaboration and knowledge sharing
- Experimenting with new technologies and methodologies in their projects
- Following industry trends and updates through newsletters and blogs
- Engaging in pilot projects to test new solutions before full implementation
- Networking with peers to share experiences and best practices

Client portrait (Regulated Industries)

Job titles

- Compliance Officers
- Risk Managers
- Data Protection Officers
- IT Security Managers
- Chief Compliance Officers (CCOs)
- Legal Advisors
- Internal Auditors

Demographics

- Age: 35-60 years old
- Location: Major cities with significant corporate presence
- Education: Advanced degrees in Law, Compliance, Cybersecurity, or related fields; many hold relevant certifications (e.g., CISA, CRISC).
- Income Level: From UAH 50,000 to UAH 200,000 monthly

Interests

- Regulatory Compliance and Data Protection
- Risk Assessment and Management
- Privacy Technologies and Solutions
- Networking with compliance and regulatory professionals
- Participation in industry regulatory bodies and associations
- Staying updated on regulatory changes and best practices
- Legal and Ethical Considerations in Data Protection
- Crisis Management and Incident Response Planning
- Data Governance and Information Management

Pain Points

- Navigating complex regulatory frameworks and compliance standards
- Protecting sensitive data and maintaining customer trust
- High stakes for compliance leading to potential penalties and reputational damage
- Need for robust privacy measures to meet regulatory requirements
- Pressure to implement personal data protection solutions that align with compliance mandates
- Difficulty in communicating compliance needs to technical teams
- Challenges in keeping up with rapid changes in regulations and technology
- Resource constraints in maintaining compliance and privacy measures

Behavior

- Regularly conducting compliance audits and assessments
- Engaging with content related to regulatory changes and best practices
- Attending industry conferences and seminars focused on compliance and privacy
- Collaborating with legal and compliance teams to ensure alignment on privacy measures
- Utilizing professional networks to share insights and strategies on compliance challenges
- Participating in training sessions to stay updated on regulatory requirements
- Following industry news and updates through specialized publications and websites
- Engaging in discussions on compliance forums and online communities

EY | Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories.

All in to shape the future with confidence.