This table provides information on the role of the data protection officer (DPO) in evaluating the data protection controls of Articles 1 to 99 of the GDPR.

Article	Outline/summary	Tasks of the DPO
1	GDPR addresses the protection and free movement of "personal data," defined in article 4 as "any information relating to an identified or identifiable natural person ('data subject').	N/A
2	GDPR applies to "the processing of personal data wholly or partly by automated means..." (Essentially, IT systems, applications, and networks) and in a business or organizational context (private home uses are not covered).	N/A
3	GDPR applies to the processing of personal data for persons in the European Union regardless of whether processed in the EU or elsewhere.	N/A
4	Data protection-related terms are formally defined in the GDPR.	N/A
5	GDPR requires that personal data be: a. Processed lawfully, fairly, and transparently b. Collected for specified, explicit, and legitimate purposes only c. Adequate, relevant, and limited to what is necessary d. Accurate e. Kept no longer than needed f. Processed securely and protected against unauthorized use	The DPO should: • Evaluate the processing activities (including the data processing records) of the organization • Review applicable laws to ensure that data is processed lawfully • Ensure that data is validated to ensure accuracy • Review the data retention policy and data destruction procedures • Review processes to ensure data integrity and confidentiality
6	The GDPR states that personal data processing is lawful only if:	The DPO should ensure that the organization:

	a. Consented by the data subject for specific purpose(s) b. Required by a contract to which the data subject is party c. Necessary for legal compliance d. Necessary to protect the vital interests of the data subject e. It is in public interest f. Necessary for the protection of personal data of the data subject, particularly when the data subject is a child **Note:** There are several detailed and explicit requirements concerning lawful processing (see the GDPR, Article 6 *Lawfulness of processing*). Note also that EU member states may impose additional rules.	• Has identified and documented the grounds for lawful processing of personal data and the period of storage for data required for the fair processing notice • Complied with Article 29 when data is used for secondary purposes • Has established business requirements to limit and protect personal data • Has implemented security controls to mitigate unacceptable risks that cannot be avoided or shared • Has covered personal data processing in the assessment and treatment of risks
7	Where applicable, the controller must provide the data subject with the consent for processing personal data, which must be freely given, and can be withdrawn easily at any time.	The DPO should ensure that the organization has: • Established mechanisms which allow requesting consent for processing • Established procedures for consent withdrawal • Included the name of the organization, the processing activities, withdrawal information, and the purpose of the data processing in the consent request • Informed the data subjects that the consent may be withdrawn • Deployed procedures that demonstrate or provide evidence that the consent has been obtained

		• Recorded the consents obtained and maintained the documented agreements with each data subject • Recorded information such as who consented, when they consented, what the data subject was told at that time, how the data subject consented, etc.
8	The controller must obtain consent from the holder of parental responsibility prior to processing personal data of a child below the age of 16 years.	The DPO should ensure that the organization: • Establishes mechanisms for obtaining consent from the holders of parental responsibility for the processing of personal data of children under the age of 16 • Takes into account the available technology while verifying that the consent is given by the holder of parental responsibility over the child
9	Special restrictions apply to particularly sensitive data concerning a person's race, political opinions, religion, sexuality, genetic data, and other biometrics. The processing of such information is *prohibited* by default *unless* explicit consent is given or processing is necessary (as defined in the Article).	The DPO should ensure that the organization: • Identifies where sensitive data may be processed • Obtains explicit consent for factors to be considered in the design of systems, applications, and business processes • Considers if any additional provisions that are related to the processing of personal data under Member State law apply • Pays attention to national developments as Member States have a broad right to impose further conditions and restrictions especially when processing genetic, health, or biometric data

10	The controller must process personal data relating to criminal convictions and offenses or related security measures only under the control of official authorities or authorized by Union or Member State law.	The DPO should ensure that the organization: • Complies with any Member State law requirements if data relating to criminal convictions or offenses are processed • Considers if background checks are necessary to be conducted, credit or fraud risk, profiling, etc.
11	The controller does not need to apply the steps for identifying the data subject if the purpose of personal data processing does not require the identification.	The DPO should ensure that the organization: • Evaluates if it really *needs* to know a data subject's identity
12	Communications with data subjects must be transparent, clear, and easily understood.	The DPO should ensure that the organization: • Establishes mechanisms that allow the data subjects to inquire in relation to their own personal data • Responds punctually (in any event within one month) and keeps records of such communications • Considers the best way to provide information in a clear and intelligible manner
13	When personal data are collected, data subjects must be provided with information such as details of the controller and the data protection officer, the purpose of processing, whether their data will be exported (especially outside the EU), how long the data will be held, their rights and how to inquire or complain, etc.	The DPO should ensure that the organization: • Defines and implements procedures for the provision of fair information regarding the processing of personal data, information on the data controller, and purposes for processing the data
14	Similar requirements to Article 13 apply if personal data is obtained indirectly (e.g., a commercial mailing	The DPO should ensure that the organization:

	list); data subjects must be informed at latest within one month and on the first communication with them.	• Updates notice where group companies are obligated to provide notices on behalf of a third party • Considers any circumstances of how information notices may be provided to the data subjects where data processed by a group organization has not been provided to the organization by the data subjects themselves
15	Data subjects have the right to obtain information on whether the organization processes their personal data, the purpose of processing, to whom it has been or may be disclosed, etc. Data subjects should be *informed* of their right to request rectification or erasure of their personal data or restriction of processing. Data subjects have the right to obtain a copy of their personal data.	The DPO should ensure that the organization: • Allows the data subject to obtain a copy of their own data (again implying the need for identification and authentication before acting on such requests) • Informs the data subjects of their right to request rectification or erasure of personal data or restriction of processing
16	Data subjects have the right to have their personal data corrected, completed, and clarified.	The DPO should ensure that the organization: • Designs and implements mechanisms to check, edit, and extend stored data, with various controls concerning identification, authentication, access, validation, etc.
17	Data subjects have the right to be forgotten, that is to have their personal data erased and no longer processed.	The DPO should ensure that the organization: • Allows the data subject to request the erasure of their personal data • Designs and implements mechanisms to erase data

		• Has the personnel and suppliers or contractors who may receive requests for data erasure recognize them and know how to handle them
18	Data subjects have the right to obtain restriction of the processing of their personal data.	The DPO should ensure that the organization: • Has designed a system, method, or mechanism to identify the specific data that is to be restricted and implement new handling or processing rules
19	The controller must communicate to the data subjects any action taken regarding the rectification or erasure of personal data or restriction of processing.	The DPO should ensure that the organization: • Has designed and implemented a mechanism for informing the data subjects
20	Data subjects have the right to receive their personal data in a structured and machine-readable format to pass to a different controller.	The DPO should ensure that the organization: • Limits the extracted data to the identified and authenticated person(s) concerned, and is communicated securely and encrypted
21	Data subjects have the right to object to processing of their personal data being used for direct marketing purposes.	The DPO should ensure that the organization: • Has designed a system, method, or mechanism to identify the data that is not to be processed and implement new handling or processing rules • Uses automated means for online services
22	Data subjects have the right not to be subject to decisions based on automated processing of their personal data.	The DPO should ensure that the organization: • Has designed profiling and decision-making support systems involving personal data that allow manual review and overrides, with

		the appropriate authorization, access and integrity controls, etc. • Considers how the rights can be met through a self-service option, wholly or partly • Has implemented consent mechanisms and has established mechanisms to re-evaluate the processing decisions, through human interventions, for exclusively automated processing
23	National laws may modify or override various rights and restrictions for national security and other purposes.	The DPO should ensure that the organization: • Has designed a legally sound manual process to assess and handle such exceptional situations
24	The controller (generally the organization that owns and benefits from processing of personal data) is responsible for implementing appropriate data protection controls (including policies and codes of conduct) considering the risks, rights, and other requirements within and perhaps beyond the GDPR.	The DPO should ensure that the organization: • Has implemented a suitable, comprehensive mesh of data protection controls, policies and procedures, as well as technical, physical, and other controls addressing the risks and compliance obligations • Has designed a structured, systematic approach to data protection • Has integrated data protection with ISO/IEC 27001 (if implemented) and other aspects, such as compliance and business continuity management • Has trained their top management on the GDPR-related requirements and the impact of not complying with these requirements

		• Has distributed the responsibilities and the financial budget for the GDPR compliance • Has reviewed reports related to data protection governance
25	Taking account of risks, costs, and benefits, there should be adequate protection for personal data by design and by default.	The DPO should ensure that the organization: • Has the support and involvement of the management • Has allocated the resources necessary to design, deliver, implement, and maintain the data protection arrangements • Has considered data protection by design such as the specification, design, development, operation, and maintenance of data protection-related systems and processes, including relationships and contracts with third parties • Has implemented internal policies and technical and organizational measuring techniques: ▷ Related to matters such as pseudonymization, transparency, and access to data ▷ That offer insurance that only personal data that need to be processed will be processed (related to the amount of the gathered data, expansion of the process, the duration of its storage and its accessibility) ▷ That guarantee that personal data will be accessible only by the authorized persons

26	Where organizations are jointly responsible for determining and fulfilling data protection requirements, they must clarify and fulfill their respective roles and responsibilities.	The DPO should ensure that the organization: • Has reviewed to see if the group organization is a joint controller whether it has an intra-group arrangement of customer or service provision • Has jointly investigated and resolved data protection incidents, breaches, or access requests, achieving and maintaining an assured level of GDPR compliance • Has respected consented purposes for which personal data was initially gathered, regardless of where it ends up
27	Organizations outside Europe must formally nominate data protection representatives inside Europe if they meet certain conditions (e.g., they routinely supply goods and services to, or monitor, European citizens).	The DPO should ensure that the organization: • Has identified non-EU group companies that need to have an EU delegate and has ensured they have the right delegate assigned in the right EU country • Has appointed in writing a representative who is designated to represent the controller or the processor to the supervisory authorities and data subjects regarding all GDPR compliance issues.
28	If an organization uses one or more third parties to process personal data (referred to as processors), it must *ensure* that they are also compliant with GDPR.	The DPO should ensure that the organization: • Has cooperated with the processor who has the necessary knowledge and experience to implement technical and organizational measures • Has cooperated with the processor who is governed by a contract or other legal act

		• Has established a process that verifies whether the processor has acted and processed personal data according to the contract or the legal act
29	Processors must only process personal data in accordance with instructions from the controller and applicable laws.	The DPO should ensure that the organization: • Has secured, controlled, and managed the personal data • Has established procedures that provide instructions on how to process personal data by not infringing the GDPR and other legal requirements • Has identified whether the authorized persons for processing are following the instructions of the controller and processor • Has established procedures that enable the authorized persons to process personal data by not following instructions of the controller and processor if the Union or the Member State law requires to do so
30	Controllers must maintain records of processing activities, the purposes of processing, categories of data subjects and personal data, etc.	N/A
31	Organizations must cooperate with the authorities, such as data protection authorities.	The DPO should ensure that the organization: • Has established policies that require effective cooperation with supervisory authorities • Has passed immediately to him or her the requests for assistance from supervisory authorities

		• Maintains contact with relevant authorities
32	The controller and processor must implement technical and organizational measures to ensure the protection of personal data.	The DPO should ensure that the organization: • Secures, controls, and manages the personal data it processes by means of pseudonymization and encryption, by ensuring the confidentiality, integrity, and availability of data, etc. • Has established procedures that provide instructions on how to process personal data by not infringing the GDPR and other legal requirements • Has identified whether the authorized persons for processing are following the instructions of the controller and processor • Has established procedures that enable the authorized persons to process personal data by not following instructions of the controller and processor, if the Union or the Member State law requires to do so
33	Personal data breaches must be reported to the relevant authorities promptly (within three days of becoming aware of the breach unless delays are justified).	The DPO should ensure that the organization: • Has established channels that enable appropriate reporting of data breaches to the supervisory authority within a time frame of 72 hours • Has established policies that require the processor to notify the controller without undue delay after becoming aware of a data breach • Has established procedures to ensure a quick, effective, and

		orderly response to data breaches • Has established a system to assess whether the data breach shall be classified as an infringement of data subjects rights and freedoms • Has established a system that detects the root cause of the data breach • Has designed and implemented an incident response plan
34	If a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the organization must communicate the breach to the data subjects without undue delay.	The DPO should ensure that the organization: • Has established a channel for communication with the data subject in case of a personal data breach • Has communicated the data breach to the data subject in a clear and plain language in the past • Has established policies that require the protection of personal data as required by the GDPR and other relevant legislation • Has established data breach response policies • Has prepared template letters and conducted rehearsals regarding data breaches
35	The organization must carry out a data protection impact assessment (DPIA) for processing that is likely to result in a high risk to the rights and freedoms of data subjects. The DPIA must be conducted prior to the processing, particularly where new technologies, systems, or arrangements are being considered.	The DPO should ensure that the organization: • Has established procedures for the conduct of a DPIA when necessary • Has identified, assessed, and treated personal data security risks, including data protection and compliance risks

		• Has established and maintains risk registers
36	The organization must consult the supervisory authority prior to processing if the DPIA indicates that the processing would result in a high level of risk to the rights and freedoms of data subjects.	The DPO should ensure that the organization: • Has reported the DPIA results to the supervisory authority when the risk level is considered high • Has established a process that defines how frequently the processing of personal data should be reviewed • Has established procedures that require revision of the processing of personal data when new risks arise
37	A data protection officer must be formally designated under specified circumstances for organizations such as public bodies, those which regularly and systematically monitor people on a large scale, or those performing large-scale processing of sensitive personal data relating to criminal records.	N/A
38	The data protection officer must be supported by the organization and engaged in data protection matters.	The DPO should ensure that the organization: • Has established policies that require him or her to get properly involved and in a timely manner in all issues related to the protection of personal data • Has determined ways of supporting him or her with the needed resources such as the staff, financial resources, and panel support
39	The data protection officer must offer advice on data protection matters, monitor compliance, liaise with the authorities, act as a contact	The DPO should ensure that the organization:

	point, address data protection risks, and so on.	• Has utilized a program related to the training of employees for data protection • Has utilized a policy that foresees the time that training and refresher courses should be held, and indicates when the training has been completed
40	Various authorities, associations, and industry bodies are anticipated to draw up codes of conduct elaborating on the GDPR and data protection, offer them to be formally approved (by an unspecified mechanism) and, where appropriate, to implement their own compliance mechanisms.	The DPO should ensure that the organization: • Has established policies that encourage the drawing up of codes of conduct intended to contribute to the proper application of the GDPR
41	The bodies behind codes of conduct are required to monitor compliance (by their members), independently and without prejudice to the legal and regulatory compliance monitoring conducted by national authorities.	The DPO should ensure that the organization: • Has established a policy that requires the monitoring of a compliance process with codes of conduct to be carried out by a body that has an appropriate level of expertise and is accredited
42	Voluntary data protection certification schemes offering compliance seals and marks (valid for three years) are to be developed and registered.	N/A
43	Certification bodies that award compliance seals and marks should be competent and accredited for this purpose. The European Commission may impose technical standards for certification schemes.	The DPO should ensure that the organization: • Has chosen an accredited certification body approved by the supervisory authority
44	International transfers and processing of personal data must fulfill the requirements laid down in subsequent GDPR Articles.	N/A

45	Data transfers to countries whose data protection arrangements (laws, regulations, official compliance mechanisms) are deemed adequate by the European Commission do not require official authorization or specific additional safeguards.	The DPO should ensure that the organization: • Has mapped and reviewed the international data flow: ▷ The data flow of intra-group ▷ EEA group company controller exporting to a controller or a processor outside of the EEA needs an extra-group data flows ▷ An EEA group which is importing as a controller or a processor needs extra-group data flows ▷ Considers the functions of the existing data transfer mechanism and review if they are appropriate ▷ The whitelisted countries remain so until a change is required from the commission review (Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay).
46	Data transfers to countries whose data protection arrangements (laws, regulations, official compliance mechanisms, etc.) are *not* deemed adequate by the European Commission but meet certain other criteria require additional safeguards.	The DPO should ensure that the organization: • Has implemented and ensured the adequacy of data protection controls before transferring personal data to a third country, e.g., suitable contractual clauses and compliance activities • Has implemented a legally binding and enforceable instrument between public authorities or bodies or binding corporate rules

		• Has included essential principles and enforceable rights providing appropriate safeguards for transfers or categories of data transfers to personal character to enterprise rules • Has implemented a code of conduct in accordance with Article 40 which includes a binding and enforceable undertaking by the manager or subcontractor to apply the appropriate safeguards, including rights of the person concerned in the country of destination
47	Supervisory authorities must approve legally binding data protection rules permitting transfers to non-approved countries.	The DPO should ensure that the organization: • Has identified their need to transfer personal data to non-approved countries
48	Requirements on European organizations from authorities outside Europe to disclose personal data may be invalid unless covered by international agreements or treaties.	The DPO should ensure that the organization: • Has identified authorities outside Europe that have requirements to disclose personal data, determine if these are valid, and if they are covered by international agreements, if any
49	Conditions apply to personal data transfers to non-approved countries, e.g., explicit consent by the data subjects.	The DPO should ensure that the organization: • Has identified non-approved countries where data needs to be transferred, if any, and ensure the obtainment of explicit consent from the data subjects if needed
50	Supervisory authorities must cooperate and provide assistance on the protection of personal data.	The DPO should ensure that the organization: • Has identified supervisory authorities that it needs to

		cooperate with in matters of data protection
51-59	These GDPR articles concern the competence, tasks, and powers of supervisory authorities.	The DPO should ensure that the organization: • Is familiar with the comprehensive tasks and powers of the supervisory authorities • Understands the lead-authority system in case cross-border processing is to be carried out
60-76	These GDPR articles concern cooperation, mutual assistance, and joint operations between the lead supervisory authority and the other supervisory authorities concerned.	N/A
77-81	Data subjects have the right to lodge complaints with supervisory authorities.	N/A
82	Any person damaged by infringements of the has the right to receive compensation from the controller or processor.	The DPO should ensure that the organization: • Has informed the contracted negotiator about the default position of each controller which is liable for the entire damage to a data subject
83	Administrative fines imposed by supervisory authorities must be “effective, proportionate and dissuasive.” Various criteria are defined. Depending on the infringements and circumstances, fines may reach 20 million EUR or up to 4% of total worldwide annual turnover for the previous year, whichever is higher.	The DPO should ensure that the organization: • Has conducted a GDPR compliance gap analysis so that areas of most material non-compliance are identified • Has conducted a GDPR compliance gap analysis in order to prioritize mitigating steps, especially in relation to high-risk processing activities • Has re-evaluated insurance agreements • Has evaluated the liability exposure under existing

		customer, partner, and supplier arrangements • Has evaluated contract exclusion clauses and liability limitation
84	Other penalties may be imposed. They too must be "effective, proportionate and dissuasive."	N/A
85	Member States must reconcile the right to the protection of personal data with the right to freedom of expression, journalism, academic research, etc. through suitable laws.	The DPO should ensure that the organization: • Has identified, assessed, and treated risks where personal data is involved
86	Personal data in official documents may be disclosed if the documents are formally required to be disclosed under 'freedom of information' – type laws.	The DPO should ensure that the organization: • Has redacted, where possible, personal or other sensitive information which will be disclosed
87	Member States may impose further data protection controls for national ID numbers.	The DPO should ensure that the organization: • Has implemented encryption and other data protection controls since national ID numbers may be used as secret personal authenticators, in which case they must remain confidential to reduce the risk of identity theft
88	Member States may impose further constraints on corporate processing and use of personal data about employees, e.g., to safeguard human dignity and fundamental rights.	The DPO should ensure that the organization: • Has identified employment laws that may intersect with the GDPR and data protection
89	Where personal data are to be archived, e.g., for research and statistical purposes, the data protection risks should be addressed through suitable controls	N/A

	such as pseudonymization and data minimization where feasible.	
90	Countries may enact additional laws concerning workers' secrecy and data protection obligations.	The DPO should ensure that the organization: • Has identified employment or secrecy laws that may intersect with the GDPR and data protection principles
92-99	These articles concern how GDPR is being enacted by the EU.	The DPO should ensure that the organization: • Complies with applicable data protection laws and regulations