Mapping between GDPR (the EU General Data Protection Regulation) and ISO27k

Release 1 November 2016

Executive summary

The European Union (EU) General Data Protection Regulation (GDPR) - currently being introduced across Europe and beyond ahead of the May 2018 final implementation deadline - mandates numerous privacy arrangements and controls designed to protect personal data, many of which are also recommended by ISO/IEC 27001:2013, ISO/IEC 27002:2013 and other "ISO27k" standards. Organizations that currently have an ISO27k ISMS (Information Security Management System) are therefore likely to have many of the GDPR requirements in place already but may need to make some adjustments. Others may choose to implement an ISO27k ISMS as an overarching framework to manage privacy and personal information as part of the broader management of information risks, information security and related compliance, incident management and business continuity issues.

This document maps between the GDPR and ISO27k in the particular context of private/non-governmental organizations subject to GDPR.

ISO27001security.com, the ISO27k Forum and the ISO27k Toolkit

The website has been running since 2005 as a *free* public information resource concerning the ISO/IEC 27000-series information risk and security management standards ("ISO27k"). It is not an official ISO/IEC site, but an unofficial community project supporting users of the ISO27k standards.

The ISO27k Forum is a non-commercial Google Group (email reflector) linking over 3,000 users of the ISO27k standards from around the world. As this is a practitioners' forum, we discuss all manner of practical ISO27k matters there. Membership is *free* but we ask you to declare your interest in ISO27k when you join as a simple means to block the robotic spammers. Overt commercials and off-topic stuff is banned, enabling us to maintain a very high signal-to-noise ratio and a friendly, supportive community atmosphere.

The ISO27k Toolkit is a *free* collection of materials donated or created by members of the ISO27k Forum to help fellow practitioners. This mapping document demonstrates the power of crowdsourcing.

Disclaimer

This is not legal advice, nor is it information risk, information security or privacy advice. This generic high-level document is provided purely for informational or general guidance purposes. You need to interpret and adapt it for your own unique situation, and if GDPR applies to your organization, you should definitely seek competent legal and other professional advice concerning the adequacy and suitability of your particular security controls and other privacy arrangements. Don't take our word for anything or blame us for the inevitable errors and omissions: we're simply trying to help.

Copyright

The mapping

ISO27k controls without the prefix 'A' are in the main body of ISO/IEC 27001:2013. Those prefixed with 'A' are listed in Annex A of ISO/IEC 27001:2013 and are explained in more detail in ISO/IEC 27002:2013. Further ISO27k standards fill-in various supplementary details (*e.g.* ISO/IEC 27005 on information risk management and ISO/IEC 27018 on privacy in cloud computing), while other ISO and non-ISO standards and resources provide lots more information, and in some case recommend alternative or complementary approaches and controls.

GDPR		ISO27k	
Article	Outline/summary	Control	Notes
1	GDPR concerns 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'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".	A.18.1.4 *etc*.	The ISO27k standards concern information risks, particularly the management of information security controls mitigating unacceptable risks to organizations' information. In the context of GDPR, privacy is largely a matter of securing people's personal information, particularly sensitive computer data. The ISO27k standards specifically mention compliance obligations relating to the privacy and protection of personal info (more formally known as Personally Identifiable Information - PII - in some countries) in control A.18.1.4.
2	GDPR concerns "the processing of personal data wholly or partly by automated means ...." (essentially, IT systems, apps and networks) and in a business or corporate/organizational context (private home uses are not in scope).	Many	ISO27k concerns information in general, not just computer data, systems, apps and networks. It is a broad framework, built around a 'management system'. ISO27k systematically addresses information risks and controls throughout the organization as a whole, including but going beyond the privacy and compliance aspects.
3	GDPR concerns personal data for people in the European Union whether is it processed in the EU or elsewhere	A.18.1.4 *etc*.	ISO27k is global in scope. Any organization that interacts with people in the European Union may fall under GDPR, especially of

GDPR		ISO27k	
Article	Outline/summary	Control	Notes
			course if they collect personal info.
4	GDPR privacy-related terms are formally defined here.	3	ISO/IEC 27000 defines most ISO27k terms including some privacy terms. Many organizations have their own glossaries in this area. **Check that any corporate definitions do not conflict with GDPR.**
Chapter I **General provisions**			
5	Personal data must be: (a) processed lawfully, fairly and transparently; (b) collected for specified, explicit and legitimate purposes only; (c) adequate, relevant and limited; (d) accurate; (e) kept no longer than needed; (f) processed securely to ensure its integrity and confidentiality. [This is the latest incarnation of the original OECD principles published way back in 1980 <tips hat>.]	6.1.2, A.8.1.1 A.8.2 A.8.3 A.9.1.1 A.9.4.1 A.10 A.13.2 A.14.1.1 A.15 A.17 A.18 ... in fact almost all!	Business processes plus apps, systems and networks must adequately secure personal information, requiring a comprehensive suite of technological, procedural, physical and other controls … starting with an assessment of the associated information risks. See also 'privacy by design' and 'privacy by default' (Article 25). In order to satisfy these requirements, organisations need to know where personal info is, classify it and apply appropriate measures to address (a)-(f).
	The "controller" is accountable for all that.	5 A.6.1.1	Although not stated as such, accountability is an important concept within the 'Leadership' section of ISO/IEC 27001.

GDPR		ISO27k	
Article	Outline/summary	Control	Notes
6	Lawful processing must: (a) be consented to by the subject for the stated purpose; (b) be required by a contract; (c) be necessary for other compliance reasons; (d) be necessary to protect someone's vital interests; (e) be required for public interest or an official authority; and/or (f) be limited if the subject is a child. *Note: there are several detailed and explicit requirements concerning lawful processing - see GDPR!* *Note also that EU member states may impose additional rules.*	6.1.2 A.14.1.1 A.18.1.1 *etc.*	This should also be covered in the assessment and treatment of information risks. It will influence the design of business processes/activities, apps, systems *etc*. (*e.g.* it may be necessary to determine someone's age before proceeding to collect and use their personal info). These are business requirements to limit and protect personal information: *many* security controls are required in practice to mitigate unacceptable information risks that cannot be avoided (by not collecting/using the data) or shared (*e.g.* relying on some other party to get consent and collect the data - a risk in its own right!).
7	The data subject's consent must be informed, freely given and they can withdraw it easily at any time.	A.8.2.3 A.12.1.1 A.13.2.4 ? A.18.1.3 6.1.2 A.14.1.1 A.8.3.2 A.13.2 *etc.*	There is a requirement to request informed consent for processing (otherwise stop!) and to be able to demonstrate this. Procedures need to be in place for this and records demonstrating the consent must be protected and retained. Withdrawal of consent implies the capability to locate and remove the personal info, perhaps during its processing and maybe also from backups and archives, plus business processes to check and handle requests.
8	Special restrictions apply to consent by/for children.	See Article 7	These special restrictions apply primarily at the time information is gathered (*e.g.* getting a parent's consent).
9	Special restrictions apply to particularly sensitive data concerning a	A.8.2.1	See 7 above. It is important to identify where sensitive data may

GDPR		ISO27k	
Article	Outline/summary	Control	Notes
	person's race, political opinions, religion, sexuality, genetic info and other biometrics *etc*. Processing of such info is *prohibited* by default *unless* consent is given *and* processing is necessary (as defined in the Article).	A.8.2.3 A.14.1.1	be processed, whether that is 'necessary' in fact, and to obtain explicit consent - factors to be considered in the design of systems, apps and business processes.
10	Special restrictions also apply to personal data concerning criminal convictions and offenses.	A.7.1 A.8.2.1 A.8.2.3 6.1.2 A.14.1.1 A.7.1 *etc*.	Any use of this information should be identified and only processed in specific circumstances. Such information should preferably not be retained except by the authorities … but may be needed for background checks, credit/fraud risk profiling *etc*.
11	Some restrictions don't apply if a person cannot be identified from the data held.	A.8.2.1 A.8.2.3 6.1.2 A.14.1.1 *etc*.	Avoiding information risks (by NOT knowing who the subjects are) is a good option, where feasible: does the business really *need* to know a person's identity or will aggregate info/statistics suffice?
Chapter III **Rights of the data subject**			
12	Communications with data subjects must be transparent, clear and easily understood.	A.12.1.1 A.14.1.1 A.16 *etc*.	See above. This affects the wording of web forms, notifications, telephone scripts *etc*. plus the processes. It may also be relevant to incident management *i.e.* mechanisms allowing people to enquire or complain in relation to their own personal information (implying a means to identify and authenticate them), for responding promptly, and for keeping records of such comms (*e.g.* to limit or charge for excessive requests)

GDPR		ISO27k	
Article	Outline/summary	Control	Notes
13	When personal data are collected, people must be given (or already possess) several specific items of information such as details of the data "controller" and "data protection officer", whether their info will be exported (especially outside the EU), how long the info will be held, their rights and how to enquire/complain *etc.*	A.8.2.1 A.8.2.3 A.12.1.1 A.14.1.1 A.16 *etc*.	Procedures for the provision of fair processing information, information on the data controller and purposes for processing the data need to be defined and implemented. This relies in part on identifying where personal info is in use.
14	Similar notification requirements to Article 13 apply if personal info is obtained indirectly (*e.g.* a commercial mailing list?): people must be informed within a month and on the first communication with them.	A.8.2.1 A.8.2.3 A.12.1.1 A.14.1 A.16 *etc*.	See Article 13.
15	People have the right to find out whether the organization holds their personal info, what it is being used for, to whom it may be disclosed *etc.*, and *be informed of* the right to complain, get it corrected, insist on it being erased *etc*. People have rights to obtain a copy of their personal information.	A.8.1.1 A.8.2.1 A.12.1.1 A.13.2.1 A.14.1.1 *etc*.	Subject rights include being able to obtain a copy of their own info (again implying the need for identification and authentication before acting on such requests), disclosing the nature of processing *e.g.* the logic behind and the consequences of 'profiling', and info about the controls if their data are exported. It may also affect backup and archive copies. See also Article 7 on withdrawal of consent.
16	People have the right to get their personal info corrected, completed, clarified *etc.*	A.12.1.1 A.14.1 A.9 A.16? A.12.3	Implies functional requirements to check, edit and extend stored info, with various controls concerning identification, authentication, access, validation *etc*. It may also affect backup and archive copies.

GDPR		ISO27k	
Article	Outline/summary	Control	Notes
		A.18.1.3	
17	People have a right to be forgotten *i.e.* to have their personal info erased and no longer used.	6.1.2 A.14.1.1 A.9 A.16 A.12.3 A.8.3.2	This is a form of withdrawing consent (see Article 7). Implies system & process functional requirements to be able to erase specific stored info, with various controls concerning identification, authentication, access, validation *etc*. It may also affect backup and archive copies.
18	People have a right to restrict processing of their personal info.	6.1.2 A.8.2.1 A.8.2.3 A.12.1.1 A.14.1.1 A.16 A.12.3 A.18.1.1	See Articles 7, 12 *etc.* May need ways to identify the specific data that is to be restricted and implement new handling / processing rules. Note it may also affect backup and archive copies.
19	People have a right to know the outcome of requests to have their personal info corrected, completed, erased, restricted *etc*.	A.12.1.1 6.1.2 A.14.1.1 A.16 *etc*.	Informing/updating the originator is a conventional part of the incident management process, but there may be a separate or parallel process specifically for privacy complaints, requests *etc.* since the originators here are not usually employees/insiders.
20	People have a right to obtain a usable 'portable' electronic copy of their personal data to pass to a different controller.	6.1.2 A.13 A.14.1.1 A.8.3	Depending on your organisation's purpose, this may seem such an unlikely scenario in practice (low risk) that it *may* best be handled by exception, manually, without automated IT system functions. Note that the extracted data must be limited to the identified and

GDPR		ISO27k	
Article	Outline/summary	Control	Notes
		A.10 A.18.1.3 *etc.*	authenticated person/s concerned, and must be communicated securely, probably encrypted. It may also imply erasing or restricting the data and confirming this (Articles 17, 18 and 19).
21	People have a right to object to their information being used for profiling and marketing purposes.	6.1.2 A.12.1.1 A.14.1.1 A.16 A.12.3 *etc*.	See article 18. May need ways to identify the specific data that is not to be processed and implement new handling / processing rules.
22	People have a right to insist that key decisions arising from automatic processing of their personal info are manually reviewed/reconsidered.	6.1.2 A.12.1.1 A.14.1.1 A.16	Profiling and decision support systems involving personal info must allow manual review and overrides, with the appropriate authorization, access and integrity controls *etc*.
23	National laws may modify or override various rights and restrictions for national security and other purposes.	A.18.1.1	This is primarily of concern to the authorities/public bodies and their systems (*e.g*. police, customs, immigration, armed forces), but may affect some private/commercial organizations, either routinely (*e.g*. legal sector, defence industry, ISPs, CSPs, money laundering rules in financial services?) or by exception (implying a legally-sound manual process to assess and handle such exceptional situations).

GDPR		ISO27k	
Article	Outline/summary	Control	Notes
Chapter IV **Controller and processor**			
24	The "controller" (generally the organization that owns and benefits from processing of personal info) is responsible for implementing appropriate privacy controls (including policies and codes of conduct) considering the risks, rights and other requirements within and perhaps beyond GDPR.	4, 5, 6, 7, 8, 9, 10 and much of Annex A	This is a formal reminder that a suitable, comprehensive mesh of privacy controls must be implemented, including policies and procedures as well as technical, physical and other controls addressing the information risks and compliance obligations. The scale of this typically requires a structured, systematic approach to privacy. Given the overlaps, it normally makes sense to integrate or at least align and coordinate privacy with the ISO27k ISMS and other aspects such as compliance and business continuity management - in other words, it is a governance issue.
25	Taking account of risks, costs and benefits, there should be adequate protection for personal info by design, and by default.	6 and much of Annex A	There are *business* reasons for investing appropriately in privacy, including information risks and compliance imperatives, as well as implementation options with various costs and benefits: elaborating on these is a good way to secure management support and involvement, plus allocate the funding and resources necessary to design, deliver, implement and maintain the privacy arrangements. Privacy by design and by default are *examples* of privacy principles underpinning the specification, design, development, operation and maintenance of privacy-related IT systems and processes, including relationships and contracts with third parties *e.g.* ISPs and CSPs.
26	Where organizations are jointly responsible for determining and fulfilling privacy requirements collaboratively, they must clarify and fulfil their respective roles and responsibilities.	5.3 9.1 A.13.2	Organizations need to manage relationships with business partners, ensuring that privacy and other information security aspects don't fall between the cracks. This includes, for instance,

GDPR		ISO27k	
Article	Outline/summary	Control	Notes
		A.15 A.16 A.18.1	jointly investigating and resolving privacy incidents, breaches or access requests, achieving and maintaining an assured level of GDPR compliance, and respecting consented purposes for which personal info was initially gathered, regardless of where it ends up.
27	Organizations outside Europe must formally nominate privacy representatives inside Europe if they meet certain conditions (*e.g.* they routinely supply goods and services to, or monitor, Europeans).	5.3 7.5.1 A.15? A.18.1.4	This is one of many compliance formalities: the Privacy Officer (or Data Protection Officer or equivalent) should be accountable for making sure this is done correctly.
28	If an organisation uses one or more third parties to process personal info ('processors'), it must *ensure* they too are compliant with GDPR.	8.2 9.1 A.15 A.18.1.1 A.18.1.3 A.18.1.4	This applies to ISPs and CSPs, outsourced data centres *etc*., plus other commercial services where the organization passes personal info to third parties *e.g.* for marketing plus HR, payroll, tax, pension and medical services for employees. It also applies on the receiving end: service suppliers can expect to be questioned about their GDPR compliance status, privacy policies and other controls (*e.g*. any subcontractors), and to have compliance and assurance clauses/terms and liabilities included in contracts and agreements. The information risks need to be identified, assessed and treated in the normal manner, on both sides.
29	Processors must only process personal info in accordance with instructions from the controller and applicable laws.	Most	Processors need to secure and control personal info in much the same way as controllers. They may well be controllers for personal info on employees *etc*. so will hopefully have all necessary privacy arrangements in hand anyway: it's 'just' a case of extending them to cover client info, and manage privacy within

GDPR		ISO27k	
Article	Outline/summary	Control	Notes
			client relationships (*e.g.* how to handle breaches or other enquiries, incidents and issues).
30	Controllers must maintain documentation concerning privacy *e.g.* the purposes for which personal info is gathered and processed, 'categories' of data subjects and personal data *etc.*	7.5	More important formalities.
31	Organizations must cooperate with the authorities *e.g.* privacy or data protection ombudsmen.	A.6.1.3	Another formality.
32	Organizations must implement, operate and maintain appropriate technical and organizational security measures for personal info, addressing the information risks.	8.2 8.3 and most of Annex A	GDPR mentions a few control examples (such as encryption, anonymization and resilience) covering data confidentiality, integrity *and* availability aspects, plus testing/assurance measures and compliance by workers (implying policies and procedures, awareness/training and compliance enforcement/reinforcement). An ISO27k ISMS provides a coherent, comprehensive and structured framework to manage privacy alongside other information risk and security controls, compliance *etc.*
33	Privacy breaches that have exposed or harmed personal info must be notified to the authorities promptly (within 3 days of becoming aware of them unless delays are justified).	A.16 A.18.1.4	Breaches *etc.* would normally be handled as incidents within the ISMS incident management process but GDPR-specific obligations (such as the 3-day deadline for notifying the authorities) must be fulfilled. Note that losses or thefts of IT devices containing personal info are *probably* not notifiable *if* the data are strongly encrypted (but remember this is NOT legal advice!). Note also that the point the clock starts ticking is not explicitly defined: it is arguably appropriate to gather and assess the available information/evident first to determine whether or not a

GDPR		ISO27k	
Article	Outline/summary	Control	Notes
			reportable incident has actually occurred *i.e.* the clock may not start until the incident is declared genuine, not a false-alarm.
34	Privacy breaches that have exposed or harmed personal info and hence are likely to harm their interests must be notified to the people so affected 'without undue delay'.	A.16 A.18.1.4	Aside from the legal and ethical considerations and direction/guidance from the privacy authorities, there are obviously significant business issues here concerning the timing and nature of disclosure. This would normally be a part of the incident management process for serious or significant incidents, involving senior management as well as specialists and advisors. Avoiding exactly this situation and the associated business costs, disruption and aggravation is one of the strongest arguments to make privacy a corporate imperative, and to invest appropriately in appropriate preventive measures. The same point applies to other serious/significant information incidents of course.
35	Privacy risks including potential impacts must be assessed, particularly where new technologies/systems/arrangements are being considered, or otherwise where risks may be significant (*e.g.* 'profiling' defined in Article 4 as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements"). 'Significantly risky situations' are to be defined by the national privacy authorities, apparently.	6.1.2 A.6.1.3 A.8.2.1 ISO/IEC 27005 and ISO 31000	Again, there are sound business and ethical reasons to identify, assess and treat information risks (including privacy and compliance risks), aside from the GDPR obligations. Privacy-related risks should probably be included in corporate risk registers alongside various other risks. GDPR also hints at integrating the assessment of privacy risks as part of the routine risk assessment activities for business change projects, new IT systems developments *etc.*

GDPR		ISO27k	
Article	Outline/summary	Control	Notes
36	Privacy risks assessed as "high" [undefined] should be notified to the authorities, giving them the chance to comment.	6.1.2 A.6.1.3 A.8.2.1 ISO/IEC 27005 and ISO 31000	The GDPR requirement is well-meaning but vague: this might be covered in corporate policies concerning the precise definition of "high" privacy risks … but on the other hand explicit inputs from the authorities may be helpful in terms of an official position on the suitability and adequacy of proposed controls - in other words this comes down to a business risk/strategic decision by management.
37	A data protection officer must be formally identified under specified circumstances *e.g.* public bodies, organizations regularly and systematically monitoring people on a large scale, or those performing large-scale processing of sensitive personal info relating to criminal records.	5.3 A.6.1.1 A.18.1.4	Aside from GDPR obligation, the "Privacy Officer" role (or equivalent titles) is much more broadly applicable and valuable, whether full or part-time, formal or informal, notifiable or not. There are clearly many angles to privacy: a designated corporate focal point for privacy (ideally a competent privacy specialist or expert) makes sense for virtually all organizations. This is another governance issue.
38	[If formally designated] the data protection officer must be supported by the organization and engaged in privacy matters.	5.3 A.6.1.1 A.18.1.4	See above. Formalities aside, without management support and engagement with the organization, a Privacy Officer is powerless and pointless.
39	[If formally designated] the data protection officer must offer advice on privacy matters, monitor compliance, liaise with the authorities, act as a contact point, address privacy risks *etc*.	5.3 A.6.1.1 A.18.1.4	See above. The GDPR requirements would form the basis of a Privacy Officer role description.
40	Various authorities, associations and industry bodies are anticipated to draw up codes of conduct elaborating on GDPR and privacy, offer them to be formally approved (by an unspecified mechanism) and (where appropriate) to implement their own (member) compliance	5.3, A.6.1.1 A.18.1.4	Although this is a valiant attempt to add weight to industry codes, it struggles to achieve a full legal mandate … but the ethical obligation is clear: privacy is more than just a matter of strict compliance with formal, legal obligations. Aside from that, codes

GDPR		ISO27k	
Article	Outline/summary	Control	Notes
	mechanisms.		(and ISO27k standards!) offer good practice guidance, and compliance may generate commercial/marketing advantages.
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 the national authorities.	5.3 A.6.1.1 A.18.1.4	See above.
42	Voluntary data protection certification schemes offering compliance seals and marks (valid for 3 years) are to be developed and registered.	5.3 A.6.1.1 A.18.1.4	Similar schemes already exist: GDPR gives them some official recognition, on top of the commercial advantages they already exploit.
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.	5.3 A.6.1.1 A.18.1.4	This should improve the credibility and meaning of privacy seals and marks, but may also increase the costs. Since they are voluntary, whether or not to be certified, and which schemes to join, are commercial/business matters for management.
Chapter V **Transfers of personal data to third countries or international organisations**			
44	International transfers and processing of personal info must fulfil requirements laid down in subsequent Articles.	-	Preamble.
45	Data transfers to countries whose privacy arrangements (laws, regulations, official compliance mechanisms ...) are deemed adequate by the European Commission (*i.e.* compliant with GDPR) do not require official authorisation or specific additional safeguards.	A.18.1.4	Most formalities are to be handled by the Commission. Compliance involves avoiding transfers to other countries, monitoring the official lists for changes, and ensuring that suitable contracts/agreements and other privacy controls are in place as with other third party data transfers (see Article 28 especially).

GDPR		ISO27k	
Article	Outline/summary	Control	Notes
46	Data transfers to countries whose privacy arrangements (laws, regulations, official compliance mechanisms ...) are *not* deemed adequate by the European Commission (*i.e.* compliant with GDPR) but meet certain other criteria require additional safeguards.	A.18.1.4	Essentially, the organization must implement and ensure the adequacy of privacy controls before transferring personal data to such countries, and subsequently *e.g.* suitable contractual clauses and compliance activities.
47	National authorities may approve legally-binding privacy rules permitting transfers to non-approved countries.	A.18.1.4	Formalities may affect contractual terms, compliance arrangements, liabilities *etc*. Hint: it may not be worth the aggravation, risks and costs.
48	Requirements on European organizations from authorities outside Europe to disclose personal data may be invalid unless covered by international agreements or treaties.	A.18.1.4, A.16	Such situations would normally be handled by legal and regulatory compliance specialists - but may start out as incidents.
49	Yet more conditions apply to personal info transfers to non-approved countries *e.g*. explicit consent by the data subjects.	A.18.1.4	The Commission is *deliberately* making it difficult, or rather taking great care since the privacy risks are higher.
50	International authorities will cooperate on privacy	-	-
Chapter VI **Independent supervisory authorities**			
51-59	[Concern national bodies to oversee privacy.]	-	-
Chapter VII **Cooperation and consistency**			
60-76	[Concern supervisory authorities and the EU Data Protection Board.]	-	-
Chapter VIII **Remedies, liability and penalties**			
77-81	[Supervisory authorities can deal with privacy complaints.]	-	-

GDPR		ISO27k	
Article	Outline/summary	Control	Notes
82	Anyone damaged by infringements of GDPR has a right to compensation from the controller/s or processor/s.	A.18.1.4	-
83	Administrative fines imposed by supervisory authorities shall be "effective, proportionate and dissuasive". Various criteria are defined. Depending on the infringements and circumstances, **fines may reach 20 million Euros or up to 4% of total worldwide annual turnover for the previous year** if greater.	6 A.18.1.4	Such huge fines are clearly intended to be a strong deterrent, representing a significant part of the potential impact of privacy breaches *etc.* in the organization's assessment of GDPR compliance and other privacy risks.
84	Other penalties may be imposed. They too must be "effective, proportionate and dissuasive".	6 A.18.1.4	See above.
Chapter IX **Provisions relating to specific processing situations**			
85	Countries must balance privacy/data protection rights against freedom of expression, journalism, academic research *etc.* through suitable laws.	6 A.18.1.1 A.18.1.4	Issues under this Article may come down to differing legal interpretations in court, hence again there are information risks to be identified, assessed and treated where personal information 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.	6 A.18.1.1 A.18.1.4	It may be feasible to redact personal or other sensitive information instead - see ISO/IEC 27038.
87	Countries may impose further privacy controls for national ID numbers.	6 A.18.1.1 A.18.1.4	National ID numbers may be used as secret personal authenticators, in which case they must remain confidential to reduce the risk of identity theft. In effect they are sensitive personal information, implying the need for encryption and other security/privacy controls.

GDPR		ISO27k	
Article	Outline/summary	Control	Notes
88	Countries may impose further constraints on corporate processing and use of personal information about employees *e.g*. to safeguard human dignity and fundamental rights.	6 A.18.1.1 A.18.1.4	Employment laws may intersect with GDPR and privacy, further complicating compliance and altering the information risks in this area.
89	Where personal data are to be archived *e.g.* for research and statistical purposes, the privacy risks should be addressed through suitable controls such as pseudonymization and data minimization where feasible.	6 A.18.1.4	Privacy concerns remain as long as the data subjects are alive (perhaps longer if their families or communities may be impacted by breaches). Taking account of this, the information risks should be identified, assessed and treated appropriately in the normal way.
90	Countries may enact additional laws concerning workers' secrecy and privacy obligations.	6 A.18.1.1 A.18.1.4	Employment or secrecy laws may intersect with GDPR and privacy, still further complicating compliance and altering the information risks in this area.
91	Pre-existing privacy rules for churches and religious associations may continue, "provided they are brought into line with" GDPR.	A.18.1.4	Good luck interpreting this highly ambiguous Article!
Chapter X **Delegated acts and implementing acts**			
92-99	[Concern how GDPR is being enacted by the EU.]	A.18.1.1	Not relevant to an individual organization's privacy arrangements, except in as much as they need to comply with applicable laws and regulations.

The “Recitals” - extensive notes preceding the Articles in GDPR - are worth reading for additional explanation relevant to information security plus some (implicit) control requirements. For instance:

Recital 39 ends with *“Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.”* - an important requirement not entirely clear from the Articles.

Recital 49 notes (in effect) that systems and network security monitoring (*e.g*. to detect and respond to hacks, denial-of-service attacks *etc*.) is a “legitimate interest of the data controller concerned”, hence it is not unlawful to capture personal data during such activities (even without the data subjects’ explicit consent) … but this doesn’t negate the need to secure it, to declare it as one of the “purposes” and to inform system/network users that the information may be monitored for such purposes.

Recital 83 starts *“In order to maintain security and to prevent processing in infringement of this regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption.”* The information-risk-driven approach is fundamental to ISO27k.