Privacy Notice

Document type

	Website privacy notice
Language	English
Organisation	DKS Consulting GmbH
Primary contact	Rudolf-Diesel-Strasse 28, 68169 Mannheim, Germany marco.l@dks-consulting.de

Topic	Summary of key points
1. Positioning of this notice	This Privacy Notice explains how DKS Consulting GmbH collects, records, structures, stores, uses, discloses and deletes personal data when visitors use the website, submit forms, request contact, consume insights, download materials or interact with DKS in a pre-sales or business relationship context. The wording is intentionally transparent and operational rather than generic.
2. Controller identity	The controller for website-related processing is DKS Consulting GmbH, Rudolf-Diesel-Strasse 28, 68169 Mannheim, Germany. Company details: HRB 755851 - Registergericht Mannheim; Tax number 37007/22929 - VAT ID DE 143203051. Main contact: marco.l@dks-consulting.de. Dedicated privacy channel to be activated on site publication: .
3. Audience and processing scenarios	The notice is written for website visitors, prospective clients, existing business contacts, newsletter recipients if activated, webinar or event registrants if activated, job applicants if a careers flow is later activated, and business partners who contact DKS through published channels. This avoids the common mistake of publishing a privacy notice that only covers a contact form but not the wider consulting website reality.

Topic	Explanation
4. Data categories collected	- identity and business profile data such as name, company, role, business email, phone number, country, sector and message content - technical usage data such as IP address, browser type, operating system, timestamp, referring URL, viewed pages, language and device metadata - form and communication data such as enquiry details, attachments, meeting requests, follow-up notes and consent records - content engagement data such as downloads, article interactions, webinar registration details and event participation records where these features are enabled - security and audit data such as server logs, anti-spam data and abuse-prevention indicators
5. Why DKS processes personal data	- to operate and secure the website - to answer enquiries and manage pre-contractual discussions - to schedule calls, demos or consulting follow-up - to deliver requested resources such as PDFs, white papers or webinar invitations - to maintain client and partner communication history in a structured way - to improve content performance, website usability and service relevance - to comply with tax, accounting, corporate and legal obligations - to establish, exercise or defend legal claims where necessary
6. Legal bases	- Art. 6(1)(a) GDPR for consent-based activities such as optional analytics, newsletter subscription or optional marketing follow-up - Art. 6(1)(b) GDPR where processing is required to take steps at the request of the data subject before entering into a contract or to perform a contract - Art. 6(1)(c) GDPR where retention or disclosure is required by law - Art. 6(1)(f) GDPR for legitimate interests such as website security, fraud prevention, system administration, business communication management and measured improvement of content and services
7. Contact forms and direct communications	If a visitor writes through a form, email address, phone number or booking tool, DKS should explain that the information is used only to process the request, verify relevance, manage follow-up and keep a documented record of the business communication. Optional fields should remain clearly marked as optional. Mandatory fields should be limited to what is genuinely necessary for the request.

Topic	Recommended wording for DKS
8. CRM and internal operational handling	Because DKS is a consulting business, inbound enquiries may reasonably be stored in internal workflows, CRM systems, shared mailboxes, project coordination tools or secure document repositories. The notice should state this clearly. Internal access should be role-based and limited to staff, founders or authorised support providers who need the data for sales, delivery, administration, IT support or compliance.
9. Cookies, analytics and similar technologies	The privacy notice should cross-reference the Cookie Notice and explain that strictly necessary technologies support security, form delivery, consent management and website stability, while analytics or advertising technologies are activated only where the legal standard for consent is met. If DKS later activates Google Analytics, LinkedIn Insight Tag, HubSpot, embedded videos or maps, the policy should be updated before deployment.
10. Recipients and processors	Website data may be processed by host endors, email service providers, spam-filter tool embedded service providers, CRM oper ooking tools, cloud storage providers, legal or tax advisers and IT maintenance partners. DKS should only use processors under documented instructions and suitable contractual safeguards.
11. International transfers	If any service provider processes personal data outside the EEA or allows remote support access from a third country, DKS should state the transfer mechanism transparently - for example adequacy decision, SCCs, supplementary measures or another lawful transfer basis. If no such transfer occurs for a tool, the text should not imply it does.
12. Retention logic	- server logs: only as long as necessary for security, troubleshooting and system integrity - contact enquiries: until the request is closed and no further follow-up is reasonably expected, unless moved into a client or prospect file - marketing consent records: for as long as needed to evidence consent and subsequent opt-out handling - client and supplier records: for the contract term and statutory retention periods - legal and compliance records: for the applicable limitation and mandatory retention periods

Topic	Recommended wording for DKS
13. Security statement	DKS should state, in clear and non-exaggerated language, that it applies appropriate technical and organisational measures, including encrypted transport, access control, least-privilege handling, backup routines, patching, secure hosting choices, provider due diligence and case-by-case logging or anti-abuse controls. At the same time, it should openly state that no internet transmission or storage architecture can guarantee absolute security.
14. Data subject rights	- right of access - right to rectification - right to erasure, where legally applicable - right to restriction of processing - right to data portability where applicable - right to object to legitimate-interest processing - right to withdraw consent at any time for future processing - right to lodge a complaint with the competent supervisory authority
15. Supervisory authority framing	Because DKS operates from Germany, the notice should direct users to the competent German supervisory authority while also remaining understandable for DACH and international visitors. The wording should say that a complaint may be lodged with the competent authority in the place of residence, work or of the alleged infringement, without pretending to list every authority exhaustively.
16. Version control and updates	The notice should include a review date, a last-updated date and a commitment to revise the text whenever DKS adds new processing activities, tools, geographies, campaign flows or recruiting features. This avoids the credibility problem of static privacy text that no longer matches the live stack.