

FROM CONFIDENTIALITY TO ACCOUNTABILITY: REGULATING PERSONAL DATA IN CONSULTANCY AGREEMENTS UNDER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023

- Ishika Harish Das¹

Abstract

Consultancy Agreements in its simplest form means an agreement which is entered upon by the consultant and client to define the terms of services such as fees, ownership, confidentiality, intellectual property rights etc. between them. Consultants handle a wide range of personal data daily in order to perform their services effectively. In dealing with such personal data, there is a high probability that the information provided may get lost, misused or exposed. The Digital Personal Data Protection Act, 2023 ("DPDP Act") provides a legal framework for protection of personal data and distinguishes between Data Fiduciaries and Data Processors but provides limited provisions on classifying professional consultants who handle personal data. This article examines how consultants are classified and how responsibility is allocated between clients and consultants. It also examines whether conventional confidentiality clauses are sufficient to address security, breach reporting, subcontracting and data deletion. The GDPR's provisions on processor arrangements and liability provide a comparative basis for developing a functional test for identifying a consultant's role and appropriate contractual safeguards. The article maintains that although the Data Fiduciary continues to bear responsibility for processing conducted on its behalf, the consultancy agreement should expressly allocate the consultant's operational duties and related financial consequences.

Keywords: Consultancy Agreements, Confidentiality, Contractual Liability, Digital Personal Data Protection Act, Data Fiduciary, Data Processor, Data Breach, Data Protection

¹ Student, DES's Shri Navalmal Firodia Law College

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com
<https://www.ijalr.in/>

I. INTRODUCTION

Consultants are hired by the business organizations to provide specialized and professional services such as recruitment, payroll, information technology, finance, marketing and legal compliance. Though they are not employees of the organizations, their duties may require access to employee, customer or other personal data. If the consultant mishandles personal data and a breach occurs, the important question that arises is how responsibility should be divided between the client and the consultant. A POSH consultant handles complaint files, an HR professional requires access to employee records and a company secretary maintains registers. The consultant faces a combination of contractual claims, professional misconduct regulations, and limited criminal liability when that data leaks, while the client faces the regulator and the individuals suffer the consequences. The Digital Personal Data Protection Act, 2023 (“DPDP Act”)² provides a legal framework for protection and regulation of digital personal data of an individual and protects the right to privacy. The DPDP Act has introduced the concept of Data Fiduciary and Data Processor and embodied various duties and obligations on them. As per Section 2 (i) of the DPDP Act, a Data Fiduciary means any person who individually or in conjunction with other persons determines the purpose and means of processing whereas Section 2(k) defines a Data Processor as any person who processes personal data on behalf of Data Fiduciary³. However, a consultant should not automatically be considered a Data Processor merely because the agreement describes the consultant in that manner. Factors such as the nature of the services, degree of control and manner of handling personal data are relevant in determining the actual role of the consultant.

The operation and enforcement of the DPDP Act is being carried out in phases and the substantive provisions of the Act will be effective from May 13, 2027. Therefore, this article adopts a prospective approach to examine how consultant relationships may be regulated once the relevant provisions become applicable. It analyses the classification of role, allocation of responsibility for data breaches and adequacy of traditional confidentiality clauses. It insists that consultancy agreements should adequately address the statutory responsibility of the Data Fiduciary from contractual

²Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

³Digital Personal Data Protection Act, No. 22 of 2023, § 2(i), (k), India Code (2023).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com
<https://www.ijalr.in/>

and operational responsibilities of the consultant and should include specific data-protection safeguards.

II. The Statutory Framework

Prior to the DPDP Act, the Information Technology Act, 2000 provided the main statutory provisions dealing with the protection of personal data. Section 43A imposed compensation liability on a body corporate that failed to adopt reasonable security practices for sensitive personal data, while section 72A dealt with the unauthorised disclosure of personal information obtained in the course of providing services under a lawful contract⁴. These provisions, however, did not recognize a specific framework for determining the legal position of external service providers involved in processing personal data.

The DPDP Act implements a more structured approach by distinguishing between a Data Fiduciary, which determines the purpose and means of processing, and a Data Processor, which processes personal data on behalf of a Data Fiduciary⁵. Section 8 places the primary responsibility for compliance on the Data Fiduciary even when processing is carried out through a Data Processor⁶. It also requires such processing to be undertaken under a valid contract and imposes obligations relating to security safeguards, breach reporting and deletion of personal data⁷. The Act further provides for substantial financial penalties for certain failures relating to security and breach notification⁸.

The DPDP Rules, 2025 enhance these legislative requirements. Rule 6 sets out safeguards such as encryption, masking, access controls, logging and backups, and also requires appropriate contractual provisions concerning processor safeguards. Rule 7 requires breach information to be communicated to the Board without delay, followed by detailed information within seventy-two hours⁹. The rules as such do not stipulate a standardized format or an exhaustive layout for processor agreements. This

⁴Information Technology Act, No. 21 of 2000, §§ 43A, 72A, India Code (2000).

⁵Digital Personal Data Protection Act, No. 22 of 2023, § 2(i), (k), India Code (2023).

⁶Digital Personal Data Protection Act, No. 22 of 2023, § 8, India Code (2023).

⁷Id. § 8(1), (2), (5),(7).

⁸Id. §§ 8(5) - (6), 33(1), First Schedule.

⁹Digital Personal Data Protection Rules, 2025, rr. 6 - 7, Gazette of India, Extraordinary, G.S.R. 846(E) (Nov. 13, 2025).

leaves organisations with the responsibility of determining contractual safeguards that are appropriate to the nature of the consultant's services and access to personal data.

III. Role of Consultants under the DPDP Framework

The Digital Personal Data Protection Act, 2023 ("DPDP Act") distinguishes between a Data Fiduciary and a Data Processor on the basis of their functions. Section 2(i) defines a Data Fiduciary as a person who, individually or in conjunction with other persons, determines the purpose and means of processing personal data, while section 2(k) defines a Data Processor as a person who processes personal data on behalf of a Data Fiduciary¹⁰. The statutory definitions therefore focus on the nature of the processing relationship rather than merely the description used in a consultancy agreement.

In the light of the fact that consultants have different levels of engagements in processing personal data, this distinction becomes imperative. An HR consultant providing recruitment advice may have limited access to personal information, whereas a consultant maintaining employee records or processing applications may directly process such data. A similar distinction can be seen in the context of consultants assisting organizations with compliance under the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 ("POSH Act")¹¹. A consultant providing policy-drafting or awareness services may have little access to personal information, while one assisting an Internal Committee with complaints or inquiry documentation may handle names, statements, evidences and other sensitive records. Hence the actual role of the consultant needs assessment based on the actual functions performed by him.

A detailed test for determination in situations where the client determines the overall objective and wherein the consultant has the discretion over the processing has not been provided by the DPDP Act. The General Data Protection Regulation (GDPR) provides a useful comparative approach by distinguishing between essential means of processing, such as the categories of data, data subjects, duration and recipients, and

¹⁰Digital Personal Data Protection Act, No. 22 of 2023, § 2(i), (k), India Code (2023).

¹¹Sexual Harassment of Women at Workplace (Prevention, Prohibition & Redressal) Act, No. 14 of 2013, India Code (2013).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com
<https://www.ijalr.in/>

non-essential means such as particular software or technical method¹². Thus, a consultant's choice of working tools does not necessarily make the consultant a Data Fiduciary.

The position may be different where the consultant independently uses personal data for its own purpose, such as benchmarking, developing an analytical model or marketing. A separate professional assessment may also be required to identify independent legal or professional obligations with regard to retention or disclosure of information where a lawyer, chartered accountant, company secretary or other professional is engaged.

Section 2(i) further refers to determining the purpose and means "in conjunction with other persons"¹³. This may cover situations involving shared decision-making, although the DPDP Act does not expressly establish a separate category of "joint Data Fiduciaries" or provide a mechanism for allocating responsibilities between them as the GDPR does under article 26¹⁴. A classification should be undertaken activity wise as multiple processing activities may be handled by a single consultant.

Section 8(2) presents a further textual issue because it refers to engaging a Data Processor for an activity related to offering goods or services to Data Principals¹⁵. The provision does not expressly explain its application to every consultancy arrangement, particularly internal functions such as HR administration or compliance support. A deliberate contractual obligation imposed on the consultants while processing personal data on behalf of a Data Fiduciary would result in greater clarity. Accordingly, the consultant's role should be assessed by considering who determines the purpose of processing, who controls its essential aspects, whether the consultant uses the data independently and whether the consultant is subject to an independent legal or professional obligation. This functional approach provides a more reliable basis for classification than the contractual label alone.

¹²European Data Protection Board, Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR, ¶¶ 40–41 (July 7, 2021)

¹³Digital Personal Data Protection Act, No. 22 of 2023, § 2(i), India Code (2023).

¹⁴Regulation (EU) 2016/679 of the European Parliament and of the Council, art. 26(1)-(3), 2016 O.J. (L 119) 1, 47- 48

¹⁵Digital Personal Data Protection Act, No. 22 of 2023, § 8(2), India Code (2023).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com
<https://www.ijalr.in/>

IV. Allocation of Responsibility for Data Protection Breaches

Section 8 of the DPDP Act places primary statutory responsibility on the Data Fiduciary even where personal data is processed on its behalf by a Data Processor¹⁶. Outsourcing a function to a consultant therefore does not, by itself, transfer the client's statutory responsibility. The consultancy agreement can nevertheless allocate operational duties and contractual consequences between the parties.

i. Security and Breach Reporting

Consultants may access personal data through computers, email, cloud platforms or other digital systems. The consultancy agreement should therefore specify appropriate security measures, including access controls, secure authentication and restrictions on copying or transferring information. The DPDP Rules, 2025 also prescribe security-related requirements for protecting personal data¹⁷. The consultant should be required to inform the client promptly after becoming aware of an actual or suspected breach and cooperate in investigation, containment and corrective action. This is particularly important where consultants handle sensitive employee or POSH-related information. The Rules, 2025 contain requirements concerning breach communication, making timely coordination between the client and consultant important¹⁸.

ii. Third-Party Access and Deletion

Consultants may rely on subcontractors, cloud services or artificial-intelligence tools. The agreement should therefore regulate third-party access and prevent the use of personal data for unauthorized purposes. Any permitted third party should be subject to appropriate data-protection obligations. The agreement should also specify when personal data must be returned or deleted after the engagement ends, subject to applicable legal retention requirements. Clear deletion provisions reduce the risk of information remaining unnecessarily in the consultant's possession.

¹⁶Digital Personal Data Protection Act, No. 22 of 2023, § 8(1), India Code (2023).

¹⁷ Id. § 8(5), Digital Personal Data Protection Rules, 2025, r. 6, Gazette of India, Extraordinary, G.S.R. 846(E) (Nov. 13, 2025).

¹⁸Digital Personal Data Protection Rules, 2025, r. 7, Gazette of India, Extraordinary, G.S.R. 846(E) (Nov. 13, 2025).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com
<https://www.ijalr.in/>

iii. Contractual Liability

The parties may allocate financial consequences through contractual remedies and indemnities. However, a further issue may arise where persons affected by the consultant's handling of personal data are not parties to the consultancy agreement. In *M.C. Chacko v. State Bank of Travancore*, the Supreme Court reaffirmed the general principle that a person who is not a party to a contract cannot ordinarily enforce its terms, subject to recognized exceptions¹⁹. This principle is relevant where consultancy agreements impose data-protection obligations intended to protect employees, customers or other third parties who are not parties to the agreement. Sections 73 and 124 of the Indian Contract Act, 1872 provide the general framework for compensation and indemnity²⁰. Any indemnity or liability cap should, however, be drafted carefully to address serious failures such as deliberate misuse or significant security breaches.

V. Beyond Confidentiality: The Need for Specific Data Protection Obligations

Confidentiality clauses are a common part of consultancy agreements. They generally restrict consultants from disclosing or misusing information received during the engagement and remain important for protecting business information, trade secrets and private records. Confidentiality, however, is not the same as data protection. A confidentiality clause mainly controls unauthorized disclosure or use, whereas data protection covers the entire handling of personal data, including access, security, sharing, retention and deletion. A consultant may therefore cause a data-protection problem without deliberately disclosing any information.

In the case of *CPP Assistance Services Pvt. Ltd. v. Teleperformance Business Services India Pvt. Ltd.*, an external service provider was entrusted with customers personal and financial information. After an alleged data-theft incident, the Bombay High Court considered contractual mechanisms concerning inspection, preservation of relevant information and access to records, including obligations that remained operative after termination of the agreement. The case demonstrates how specific contractual safeguards can become important when personal data is processed by an

¹⁹*M.C. Chacko v. State Bank of Travancore*, (1969) 2 SCC 343, 349–50, AIR 1970 SC 500.

²⁰Indian Contract Act, No. 9 of 1872, §§ 73, 124, India Code (1872).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com
<https://www.ijalr.in/>

external service provider²¹.

For example, a consultant may accidentally send an employee database to the wrong person, leave a device containing customer information unsecured or continue to retain personal data after completing the assignment. These situations involve security or retention concerns that may not be adequately addressed by a general promise of confidentiality.

A standard confidentiality clause may also leave important practical questions unanswered. It may not specify the security measures expected from the consultant, the time within which a breach must be reported, whether subcontractors or external software may be used, or when personal data must be returned or deleted. These matters become particularly important where consultants use cloud platforms or artificial-intelligence tools while performing their services²².

The position is especially sensitive for consultants involved in POSH-related work. A consultant assisting an Internal Committee may handle complaint records, statements and information concerning the persons involved. Section 16 of the POSH Act restricts the publication or communication of information relating to such proceedings²³. A confidentiality clause can support this obligation, but the consultancy agreement should also address security, access, breach reporting and retention of the records.

The DPDP framework makes contractual clarity important because the Data Fiduciary remains responsible for processing carried out on its behalf by a Data Processor²⁴. The parties should therefore not rely only on a general statement that the consultant will comply with “applicable data-protection laws”. Instead, the agreement should contain a separate data-protection clause or schedule setting out the consultant’s specific obligations.

Such a provision may cover the permitted purpose of processing, categories of personal data, access controls, security measures, breach notification, third-party access, use of external technologies, retention and deletion. A data-processing

²¹CPP Assistance Services Pvt. Ltd. v. Teleperformance Business Services India Pvt. Ltd., Commercial Arbitration Petition (L) No. 475 of 2026, 2026:BHC-OS:3228, ¶¶ 25, 37, 41, 44 (Bom. H.C. Feb. 3, 2026).

²²Piotr Brzeziński, Personal Data Processing Contract, 13 Ius Novum 184, 184–95 (2019)

²³Sexual Harassment of Women at Workplace (Prevention, Prohibition & Redressal) Act, No. 14 of 2013, § 16, India Code (2013).

²⁴Digital Personal Data Protection Act, No. 22 of 2023, § 8(1), India Code (2023).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com
<https://www.ijalr.in/>

schedule can therefore complement the confidentiality clause without replacing it. Confidentiality should consequently be treated as one part of the contractual framework for protecting personal data, rather than as a complete substitute for specific data-protection obligations. This approach provides clearer responsibilities for both the client and consultant and is better suited to modern consultancy arrangements involving digital systems and third-party technologies²⁵.

VI. Comparative Perspective: GDPR and Lessons for India

The General Data Protection Regulation (“GDPR”) provides a useful comparative framework because it contains detailed rules governing controller-processor relationships. Article 28 requires processing by a processor to be governed by a contract specifying matters such as the purpose and duration of processing, the categories of personal data involved and the obligations of the parties²⁶.

The GDPR also imposes specific duties on processors, including following documented instructions, maintaining appropriate security measures and notifying the controller of a personal data breach without undue delay²⁷. Importantly, Article 28(10) provides that a processor who determines the purposes and means of processing is treated as a controller for that processing. Article 26 similarly recognizes joint controllership where parties jointly determine the purposes and means of processing²⁸. These provisions demonstrate the importance of examining the actual role of a consultant rather than relying only on the contractual nomenclature.

The GDPR also provides a more developed framework for liability and compensation for material or non-material damage caused by a violation of the regulation under Article 82²⁹. However, in India the DPDP Act does not follow the same compensation model and the GDPR should therefore not be directly transplanted into Indian law.

²⁵Yordanka Ivanova, *Data Controller, Processor or a Joint Controller: Towards Reaching GDPR Compliance in the Data and Technology Driven World* (Mar. 1, 2020).

²⁶Regulation (EU) 2016/679 of the European Parliament and of the Council [hereinafter GDPR], art. 28(3), 2016 O.J. (L 119) 1, 48-49.

²⁷GDPR, arts. 28(2) -(4), 29, 32, 33(2).

²⁸GDPR, arts. 26(1), 28(10).

²⁹GDPR, art. 82(1) -(5).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com
<https://www.ijalr.in/>

The main lesson for India is the need for clearer contractual and regulatory guidance. Consultancy agreements should specify the purpose of processing, security measures, breach-reporting requirements, third-party access, deletion obligations and contractual consequences. Regulatory guidance could also adopt a functional approach to role classification and clarify the position of consultants who perform different roles in relation to different processing activities.

The GDPR therefore offers India a useful comparative lesson rather than a model for direct adoption. Its value lies in demonstrating the importance of functional role classification and specific contractual obligations for organizations engaging consultants to handle personal data.

VII. A Functional Approach to Consultant Liability

A consultant's classification as a Data Fiduciary or Data Processor should be determined by the scope and nature of the circumstances rather than the nomenclature in the contract. A functional approach could give more clarity in cases where consultants work as professional providers of services, and also work with personal data.

There are some factors that are especially important. The nature and scope of access to personal data, the purpose of processing, including who chooses why the data is used, the degree of control, including who decides how it is handled, and the involvement of third parties, such as subcontractors, cloud services, and artificial intelligence technologies. These elements ought to be evaluated in light of the consultant's actual duties.

Specific inclusion of security requirement, breach reporting, access to third parties, retention and deletion, confidentiality and contractual liability should be included as mandatory clauses in the Consultancy agreements. Such provisions do not transfer the Data Fiduciary's statutory responsibility under the DPDP Act but clarify the consultant's operational duties and consequences of breach of contractual obligations. A functional approach therefore provides a practical basis for allocating consultant responsibility while maintaining the distinction between statutory and contractual

liability.

VIII. CONCLUSION:

The DPDP Act establishes a primary framework for allocating responsibility between Data Fiduciaries and Data Processors. However, the position of professional consultants requires great clarity. A consultant's role should be assessed according to the actual purpose of processing, degree of control and extent of access to personal data rather than merely the contractual nomenclature. This functional approach is particularly important where consultants exercise professional judgment or perform different functions involving personal data.

The Data Fiduciary cannot avoid its statutory responsibility merely by outsourcing data-related functions to a consultant. At the same time, consultants should not be left with undefined responsibilities. Consultancy agreements should therefore clearly address security measures, breach reporting, third-party access, retention and deletion, confidentiality and contractual liability.

The GDPR depicts the importance of detailed processor obligations and functional role classification, although its framework cannot be directly incorporated into Indian law. The DPDP framework can instead adopt these principles through appropriate guidance and contractual practices. A functional approach, supported by specific data-protection obligations, can therefore provide greater certainty and accountability. It can also help ensure that responsibility corresponds to the actual role and level of control exercised by each party, while preserving the Data Fiduciary's statutory responsibility under the DPDP Act.