FACULTY OF LAW

PUBLIC CONSULTATION SUBMISSION

on the

Draft Template for Personal Data Breach Notification

under Article 33 of Regulation (EU) 2016/679 (General Data Protection Regulation - GDPR)

Prepared in response to the European Data Protection Board's Public Consultation on the Draft Template for Personal Data Breach Notification

INTERNATIONAL LEVEL POLICY DOCUMENT

(Policy Protocol No: 02/2026)

Submitted By:

CENTRE FOR LAW AND TECHNOLOGY,
FACULTY OF LAW
SRM UNIVERSITY DELHI-NCR, SONEPAT, HARYANA

AUGUST, 2026

TABLE OF CONTENT

ABOUT THIS REPORT iii

ABOUT SRM UNIVERSITY DELHI-NCR SONIPAT, HARYANA v

ABOUT FACULTY OF LAW, SRMUH vi

ABOUT THE CENTRE vii

DETAILED ANALYSIS AND RECOMMENDATIONS 1

Notification Categories and Follow-up Notification Process……..……1

Controller's Awareness Threshold under Article 33 GDPR……..……2

Differentiation of Personal Data Categories and Identification of Sensitive Data……..…….3

Effectiveness of Technical and Organisational Measures...……..4

Assessing the Severity of Potential Adverse Effects on Data Subjects…..……5

Strengthening Guidance on Risk Assessment under Articles 33 and 34 GDPR……...6

Distinguishing Implemented and Proposed Measures……..…...7

Linking Preventive Measures to Root Causes and Identified Vulnerabilities……..……8

Ensuring Completeness of Communication Requirements under Article 34(2) GDPR...……9

Relationship between Risk Assessment and Communication to Data Subjects……..10

Development of Supplementary Implementation Guidance for Harmonised Application…..11

CONCLUDING REMARKS viii

ABOUT THIS REPORT

Personal data breach notification constitutes a fundamental component of the accountability framework established under Regulation (EU) 2016/679 General Data Protection Regulation (GDPR). Articles 33 and 34 GDPR impose complementary obligations on controllers to notify competent supervisory authorities and, where applicable, affected data subjects following a personal data breach. Effective breach notification not only enables supervisory authorities to assess risks and oversee regulatory compliance but also facilitates timely mitigation measures, promotes organisational accountability, and reinforces public trust in the processing of personal data.

Recognising the importance of ensuring a consistent and harmonised approach to breach notification across the European Union, the European Data Protection Board (EDPB) has published, for public consultation, the Draft Template for Personal Data Breach Notification under Article 33 GDPR. The proposed template seeks to establish a common notification framework capable of improving the quality, completeness, and comparability of personal data breach notifications submitted to supervisory authorities throughout the European Economic Area. By promoting greater consistency in reporting practices, the initiative represents an important step towards facilitating more coherent supervisory assessment and supporting the uniform application of the GDPR across Member States.

Given the practical significance of this initiative, the effectiveness of the final notification template will depend not only upon the information requested but equally upon the clarity of its legal concepts, the consistency of its implementation, and its practical usability for controllers operating across different sectors and organisational contexts. A harmonised notification framework should enable controllers to submit accurate, consistent, and meaningful notifications while ensuring that supervisory authorities receive sufficient information to assess the nature of the breach, its likely consequences, the risks posed to the rights and freedoms of natural persons, and the adequacy of the measures adopted in response.

The present report undertakes a detailed examination of the Draft Template through a provision-by-provision analysis of its structure, conditional logic, explanatory guidance, and reporting requirements. The assessment is conducted with reference to the notification obligations contained in Articles 33 and 34 GDPR, the accountability principle under Article 5(2), the security obligations under Article 32, and the *Article 29 Working Party Guidelines on*

Personal Data Breach Notification under Regulation (EU) 2016/679 (WP250 rev.01), as endorsed by the European Data Protection Board. The analysis further considers whether the draft template adequately promotes legal certainty, practical implementation, and harmonised supervisory practice while remaining proportionate to the objectives of the GDPR.

The recommendations contained in this report are intentionally limited to targeted refinements capable of enhancing the clarity, consistency, and practical operation of the draft template. They do not seek to modify the substantive legal obligations established under the GDPR. Instead, they primarily recommend the incorporation of concise explanatory notes, contextual tooltips, and supplementary implementation guidance to assist controllers in interpreting and completing the notification form in a consistent manner, while preserving the overall structure and objectives of the draft template.

It is in this context that the Centre for Law and Technology (CLT), Faculty of Law, SRM University Delhi-NCR, Sonipat, respectfully submits the present Report for the consideration of the European Data Protection Board (EDPB). The observations and recommendations contained herein are intended to contribute constructively to the ongoing public consultation process by identifying practical opportunities to strengthen the draft notification template in a manner that promotes greater legal certainty, enhances consistency in personal data breach notifications, and supports the harmonised application of Articles 33 and 34 GDPR across the European Economic Area. It is respectfully submitted that these recommendations may assist in the development of a robust, practical, and future-ready notification framework that facilitates effective regulatory oversight while supporting controllers in fulfilling their obligations under the GDPR.

ABOUT SRM UNIVERSITY DELHI-NCR SONIPAT, HARYANA

SRM University Delhi-NCR, Sonipat, Haryana (SRMUH) is a prestigious state private university established under the Haryana Private Universities (Amendment) Act, 2013, and is part of the renowned SRM Educational Group. Located in the Rajiv Gandhi Education City, Sonipat, SRMUH is recognized by the University Grants Commission (UGC) under section 2(f) of the UGC Act, 1956. SRM Group's commitment to academic excellence and cutting-edge research is reflected across its multiple disciplines.

The university offers over 50 multidisciplinary programs spanning Engineering & Technology, Management, Law, Science, and Humanities. With students from more than 25 states and union territories, SRMUH has rapidly risen in academic rankings, placing it among the Top 50 universities in India. Accredited with an A+ by NAAC, the university is also recognized for its excellence in IT-enabled learning by Education World. Powered by NASSCOM FutureSkills, SRMUH ensures that its curriculum aligns with the needs of a dynamic and evolving workforce.

Founded as part of SRM Group's broader objective to expand quality education across Northern India, SRMUH carries forward the legacy that began in 1969 with a small primary school. Today, the SRM Group operates 22 institutions and 4 universities across India. SRMUH strives to be a leading global educational institution, fostering the highest standards of instruction while integrating experiential learning, life skills, and social responsibility into its programs. Graduates from SRMUH are equipped not only with academic excellence but also with the ethical and leadership qualities needed to contribute to society and take on future leadership roles.

ABOUT FACULTY OF LAW, SRMUH

The Faculty of Law at SRM University Delhi-NCR, Sonipat is committed to fostering the next generation of skilled legal professionals. Recognized by the Bar Council of India (BCI), it offers a range of programs including the LL.B. (Hons.), LL.M., and five-year integrated courses such as B.B.A. LL.B. (Hons.) and B.A. LL.B. (Hons.). These programs are designed to meet the highest legal standards while being competitively priced for accessibility.

Under the leadership of Prof. Dr. Vijay Kumar Singh, Dean, and Dr. Shalini Saxena, Head of Department, the curriculum balances theoretical knowledge with practical skills, ensuring students graduate with the integrity and social sensitivity necessary to excel in the legal profession.

The faculty boasts specialized research centers, including:

- Centre for Constitutional Law and Public Policy (CCPL)
- Centre for International Law and Institutions (CILI)
- Centre for Criminal Law and Policy (CCLP)
- Centre for Corporate, Competition, and Insolvency Laws (CCCIL)
- Centre for Law and Technology (CLT)
- SRMUH Centre for Intellectual Property Rights (SCIPR)
- SRMUH Centre for Alternative Dispute Resolution (SCADR)

These centers drive research and excellence in their respective fields. The Dr. Babasaheb Ambedkar Chair on Justice further reinforces the faculty's commitment to social justice research. Active student-led initiatives, such as the Moot Court Committee and the Legal Aid Cell, enhance practical learning and community outreach, reflecting the faculty's dedication to social responsibility. With a focus on academic excellence and real-world application, the Faculty of Law at SRMUH is the ideal destination for aspiring legal professionals ready to meet the challenges of the future.

ABOUT THE CENTRE

The Centre for Law and Technology (CLT), Faculty of Law, SRM University Delhi-NCR, Sonipat is a multidisciplinary academic and research centre dedicated to examining the evolving relationship between law, technology, and public policy. Established with the objective of bridging legal scholarship and technological innovation, the Centre seeks to advance research on the legal, regulatory, and ethical implications of emerging technologies, including artificial intelligence, blockchain, quantum technologies, cybersecurity, data protection, digital governance, and the Internet of Things. Through rigorous academic research, capacity-building initiatives, policy engagement, and interdisciplinary collaboration, the Centre aims to contribute to the development of responsible, human-centric, and rights-based technology governance while promoting innovation consistent with the rule of law.

In furtherance of these objectives, the Centre actively contributes to public policy by preparing research reports, consultation responses, and policy recommendations for governmental bodies, regulatory authorities, judicial institutions, and international organisations on emerging issues relating to law and technology. The Centre seeks to support evidence-based policymaking through independent legal research grounded in constitutional values, comparative jurisprudence, and international best practices.

The Centre has also organised several national and international academic initiatives that promote interdisciplinary dialogue on technology regulation. Most notably, it organised the International Conference on "Lex Ex Machina: Interdisciplinary Dialogues for a Responsible Digital Future" on 14-15 November 2025, which brought together scholars, policymakers, regulators, judges, legal practitioners, and industry experts from jurisdictions including the United States, the United Kingdom, Romania, Australia, Rwanda, Nigeria, Sri Lanka, and Argentina. The conference reflected the Centre's commitment to fostering comparative legal scholarship, international collaboration, and meaningful engagement on contemporary issues concerning law, technology, and digital governance.

DETAILED ANALYSIS AND RECOMMENDATIONS

S.No	Section	Observation / Gap Identified	Recommendation	Rationale	Anticipated Impact
	Notification Categories and Follow-up Notification Process				
1.	**1.1 Type of Notification**	The template distinguishes between new and follow-up notifications and classifies follow-up notifications as complete, incomplete, or withdrawn. However, it does not expressly clarify whether a complete notification signifies the conclusion of the controller's investigation or the submission of all information available at the time of notification. It also does not expressly indicate that controllers may submit successive follow-up notifications where additional relevant information becomes available.	The template could be supplemented with concise explanatory guidance clarifying that a complete notification reflects the information available at the time of submission and does not necessarily indicate that the investigation has concluded. It could further clarify that controllers may submit successive follow-up notifications where additional relevant information becomes available in accordance with Article 33(4) GDPR. Such clarification may be incorporated through explanatory notes, tooltips, or accompanying implementation guidance.	Although the notification categories are defined, further clarification of their practical application would promote a consistent understanding of the notification lifecycle and reduce divergent reporting practices. The proposed clarification reflects the phased notification approach envisaged under Article 33(4) GDPR without imposing any additional reporting obligations.	The recommendation would improve legal certainty, promote greater consistency in the use of notification categories across Member States, and facilitate more harmonised supervisory practices while preserving the flexibility intended by Article 33 GDPR.

	Controller's Awareness Threshold under Article 33 GDPR				
2.	**3.1 Date and Time of the Personal Data Breach and of its Detection**	The draft template comprehensively captures the chronology of a personal data breach by recording the date and time of occurrence, the controller's awareness, the method of discovery, external notifications, and supporting timeline information. However, while the template requires controllers to specify the date and time of awareness of the personal data breach, it does not clarify the legal threshold for determining when a controller is considered to have become "aware" of a breach for the purposes of Article 33 GDPR. As the commencement of the 72-hour notification period is intrinsically linked to this concept, the absence of explanatory guidance may result in divergent interpretations and	The template should include concise guidance clarifying the legal meaning of the controller's "awareness" of a personal data breach for the purposes of Article 33 GDPR. In particular, it should distinguish the date of occurrence of the breach, the date of its detection, and the date on which the controller is deemed to have become aware of the breach. The guidance should further indicate that the assessment of awareness should be undertaken consistently with the interpretation set out in the EDPB/WP29 Guidelines. Such clarification may be incorporated through explanatory notes, enhanced tooltips, or accompanying implementation guidance.	Article 33(1) GDPR requires controllers to notify the competent supervisory authority without undue delay and, where feasible, not later than 72 hours after becoming aware of a personal data breach. While the draft template appropriately records the controller's awareness date and conditionally requires reasons for late notification where the 72-hour period has elapsed, it does not explain the legal threshold for determining when awareness arises. The Article 29 Working Party Guidelines on Personal Data Breach Notification under Regulation (EU) 2016/679 (WP250 rev.01), endorsed by the EDPB, clarify that a controller should be regarded as becoming aware when it has a reasonable degree of certainty that a security incident has occurred and that	Clarifying the concept of the controller's awareness would strengthen legal certainty, promote the consistent calculation of the 72-hour notification period, reduce divergent reporting practices, and enhance the harmonised implementation of Article 33 GDPR across Member States.

		inconsistent reporting practices across controllers and Member States.		it has resulted in personal data being compromised. Incorporating a concise explanation of this established interpretation would promote a consistent calculation of the 72-hour notification period, facilitate the uniform application of the template's conditional logic relating to late notifications, and further the EDPB's objective of harmonised breach notification practices across the European Union.	
	Differentiation of Personal Data Categories and Identification of Sensitive Data				
3.	**3.4 Categories and number of personal data records concerned**	The template comprehensively lists categories of personal data that may be affected by a breach. However, it does not distinguish between ordinary personal data, special categories of personal data under Article 9 GDPR, and personal data relating to criminal convictions and offences under Article 10 GDPR. As a result, controllers	The template should provide a clear indication of which data categories constitute special categories of personal data under Article 9 GDPR and which relate to criminal convictions and offences under Article 10 GDPR. Such clarification may be incorporated through visual indicators, explanatory notes, or tooltips accompanying the relevant data categories, without altering the existing structure of the template.	Article 33(3)(c) GDPR requires controllers to assess and report the likely consequences of a personal data breach. The nature of the affected personal data is a central factor in that assessment, particularly where the breach involves special categories of personal data under Article 9 GDPR or data relating to criminal convictions and offences under Article 10 GDPR.	Clear identification of data categories protected under Articles 9 and 10 GDPR would improve the accuracy and consistency of breach notifications, assist controllers in conducting risk assessments, and facilitate more harmonised supervisory evaluation

		particularly those with limited data protection expertise may not readily appreciate the differing legal significance of these categories when assessing the breach and its potential consequences.		While the draft template already captures these categories, it does not distinguish their legal status or significance. Providing concise explanatory guidance would assist controllers in identifying these categories correctly, support more consistent risk assessments, and promote greater harmonisation in breach notifications across Member States without imposing any additional reporting obligations.	across the European Union.
	Effectiveness of Technical and Organisational Measures				
4.	**3.5 Measures in place when the personal data breach occurred**	The draft template records the technical and organisational measures that were in place when the personal data breach occurred. However, it does not expressly invite controllers to indicate whether those measures were operational and effective in mitigating the breach, except in limited circumstances where	The template should encourage controllers to briefly indicate, where relevant, whether the technical and organisational measures identified were effective in preventing, limiting, or mitigating the impact of the personal data breach. This could be incorporated through a short explanatory prompt or tooltip within the existing narrative field, without introducing	Article 32 GDPR requires controllers to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The effectiveness of those measures is an important contextual factor in understanding how the breach occurred, assessing its likely consequences, and evaluating whether appropriate	Providing contextual information on the effectiveness of existing safeguards would improve the quality and consistency of breach notifications, assist supervisory authorities in assessing the incident more accurately, and encourage more

		technical measures are likely to have been subverted.	additional mandatory fields or reporting obligations.	safeguards were in place. While the template already records the existence of relevant measures, a brief explanation of their operational effectiveness would provide supervisory authorities with more meaningful information while avoiding any additional administrative burden for controllers.	meaningful reporting on the practical operation of technical and organisational measures.
	Assessing the Severity of Potential Adverse Effects on Data Subjects				
5.	**4.1 Likely consequences of the personal data breach and potential adverse effects on data subjects**	The template requires controllers to classify the severity of the potential impacts as Minor, Moderate, or Severe, but it does not provide any guidance or indicative criteria explaining how these classifications should be applied. This may result in inconsistent severity assessments across controllers and Member States.	The template should include concise guidance or illustrative criteria to support the assessment of the severity of the potential impacts on data subjects. Such guidance could be incorporated through explanatory tooltips or accompanying implementation guidance, clarifying that the assessment should take into account factors such as the nature and sensitivity of the personal data, the categories and vulnerability of the affected data subjects, the scale of the breach, and the likelihood and	Article 33(3)(c) GDPR requires controllers to describe the likely consequences of a personal data breach, while the GDPR adopts a risk-based approach focused on the potential impact on the rights and freedoms of natural persons. The draft template appropriately requires controllers to indicate the severity of the potential impacts but does not specify the factors that should inform that assessment. Providing concise guidance would	Providing indicative criteria for assessing severity would improve the consistency and transparency of breach notifications, facilitate more harmonised supervisory assessment, and strengthen the quality of risk evaluations under Article 33 GDPR.

			seriousness of the adverse effects on the rights and freedoms of natural persons.	promote a more consistent and objective evaluation of severity, improve the comparability of notifications across Member States, and support supervisory authorities in assessing breach notifications in a harmonised manner without increasing the reporting burden.	
	Strengthening Guidance on Risk Assessment under Articles 33 and 34 GDPR				
6.	**4.2 Assessment of the Risk to the Rights and Freedoms of Natural Persons**	The draft template requires controllers to indicate the outcome of their risk assessment and to provide a description of the methodology used. However, it does not identify the principal factors that should be considered when determining whether a personal data breach is likely to result in a risk or a high risk to the rights and freedoms of natural persons. In the absence of such guidance, controllers may adopt differing	The template could be supplemented with concise explanatory guidance identifying the principal factors that should inform the assessment of risk to the rights and freedoms of natural persons. Such guidance could indicate that controllers should consider, where relevant, factors including the nature and sensitivity of the personal data concerned, the volume of data affected, the categories and vulnerability of the affected data subjects, the ease of identification of individuals, the likelihood and severity of potential adverse	Articles 33 and 34 GDPR adopt a risk-based approach, requiring controllers to assess whether a personal data breach is likely to result in a risk or a high risk to the rights and freedoms of natural persons. While the draft template requires controllers to record the outcome of that assessment, it does not indicate the principal considerations that should inform it. The EDPB/WP29 Guidelines identify a number of relevant factors that contribute to a consistent and objective assessment of risk.	Providing indicative guidance on the factors relevant to risk assessment would promote more consistent and transparent breach notifications, strengthen the quality and comparability of controllers' risk assessments, and facilitate a more harmonised application of Articles 33 and 34 GDPR across Member States.

		approaches to risk assessment, resulting in inconsistent breach notifications and supervisory evaluation.	effects, and any mitigating technical or organisational measures. The guidance may be incorporated through explanatory notes, tooltips, or accompanying implementation guidance.	Reflecting these factors in the accompanying guidance would promote greater consistency in breach notifications and support harmonised supervisory practice without imposing additional reporting obligations.	
	Distinguishing Implemented and Proposed Measures for Addressing Personal Data Breaches				
7.	**4.3 Measures taken (or proposed to be taken) to address the personal data breach and to mitigate its possible adverse effects**	The draft template provides a single narrative field for describing the measures taken (or proposed to be taken) to address the personal data breach and mitigate its consequences. However, it does not expressly encourage controllers to distinguish between measures that have already been implemented and those that are planned or proposed for future implementation.	The template could encourage controllers to distinguish, within the existing narrative field, between measures that have already been implemented and measures that are proposed or planned for future implementation to address the personal data breach and mitigate its adverse effects. This clarification could be incorporated through an explanatory tooltip or accompanying implementation guidance without introducing additional mandatory fields.	Article 33(3)(d) GDPR requires controllers to describe both the measures taken and those proposed to be taken to address a personal data breach and mitigate its possible adverse effects. While the draft template provides a single narrative field for this purpose, distinguishing between implemented and proposed measures would improve the clarity and completeness of notifications. It would also assist supervisory authorities in assessing the controller's immediate response, ongoing remediation efforts, and planned corrective actions	Encouraging a clear distinction between implemented and proposed measures would improve the transparency and consistency of breach notifications, facilitate supervisory assessment of incident response, and promote more structured reporting while preserving the flexibility of the current template.

				without imposing any additional reporting obligations.	
	Linking Preventive Measures to Root Causes and Identified Vulnerabilities				
8.	**4.4 Measures taken (or proposed to be taken) to prevent similar personal data breach**	The draft template requires controllers to describe the measures taken or proposed to prevent similar personal data breaches in the future. However, it does not expressly encourage controllers to explain how those measures address the underlying causes or vulnerabilities identified during the investigation of the incident.	The template could encourage controllers to briefly explain how the preventive measures implemented or proposed address the underlying causes or vulnerabilities identified in relation to the personal data breach. This clarification could be incorporated through an explanatory tooltip or accompanying implementation guidance within the existing narrative field, without introducing additional mandatory fields.	The accountability principle under Article 5(2) GDPR, read together with the obligation under Article 32 GDPR to implement appropriate technical and organisational measures ensuring a level of security appropriate to the risk, requires controllers not only to respond to individual personal data breaches but also to adopt measures that effectively reduce the likelihood of recurrence. While the draft template records the preventive measures adopted, a brief explanation linking those measures to the identified causes or vulnerabilities would assist supervisory authorities in assessing whether the proposed remediation is appropriately targeted and proportionate to	Encouraging controllers to link preventive measures to the identified causes of the breach would improve the transparency, quality, and accountability of breach notifications, facilitate more effective supervisory assessment of corrective actions, and promote more meaningful organisational learning following personal data breaches.

				the incident. This would improve the quality of breach notifications without imposing additional reporting obligations.	
	Ensuring Completeness of Communication Requirements under Article 34(2) GDPR				
9.	**5. Communication to the data subjects**	The draft template requires controllers to provide the content of the communication addressed to affected data subjects but does not remind controllers of the minimum information required under Article 34(2) GDPR. Consequently, controllers may submit communications that do not fully reflect the mandatory elements prescribed by the Regulation.	The tooltip accompanying the field requesting the content of the communication to affected data subjects could include a concise reminder that the communication should comply with Article 34(2) GDPR, including, where applicable, the contact details of the data protection officer or other contact point, a description of the likely consequences of the personal data breach, the measures taken or proposed to address the breach, and recommendations to mitigate its possible adverse effects. Such clarification could be provided through an explanatory note or accompanying implementation guidance without modifying the existing structure of the template.	Article 34(2) GDPR prescribes the minimum information that must be communicated to affected data subjects where notification is required. While the draft template requests controllers to provide the content of that communication, a concise reminder of these statutory requirements would promote more complete and consistent communications, assist controllers in complying with their legal obligations, and facilitate supervisory authorities in assessing compliance with Article 34 GDPR. The recommendation does not introduce any additional reporting obligation but reinforces	Providing a reminder of the mandatory elements under Article 34(2) GDPR would improve the completeness and consistency of communications submitted with breach notifications, support controllers in meeting their legal obligations, and facilitate more efficient supervisory assessment of compliance.

				existing statutory requirements.	
	Clarifying the Relationship between Risk Assessment and Communication to Data Subjects				
10.	**5. Communication to the Data Subjects**	The draft template separately addresses the controller's assessment of the risk to the rights and freedoms of natural persons and the subsequent communication of the personal data breach to affected data subjects. However, it does not expressly remind controllers that a finding of a high risk under Article 33 GDPR will ordinarily require communication to affected data subjects under Article 34 GDPR unless one of the exceptions in Article 34(3) GDPR applies.	The template could include a concise explanatory note or tooltip clarifying that where the controller concludes that the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, communication to affected data subjects is generally required under Article 34 GDPR unless one of the exceptions set out in Article 34(3) GDPR applies. Such clarification could be incorporated through explanatory guidance without modifying the existing structure of the template.	Articles 33 and 34 GDPR establish complementary but distinct notification obligations. While the draft template separately addresses the assessment of risk and communication to affected data subjects, it does not expressly highlight the legal relationship between these provisions. A concise reminder would assist controllers in understanding the circumstances in which communication to affected data subjects is required, promote greater consistency in decision-making, and reinforce the risk-based framework established by the GDPR without introducing additional reporting obligations.	Clarifying the relationship between Articles 33 and 34 GDPR would improve the consistency of controllers' decisions regarding communication to affected data subjects, facilitate supervisory assessment of compliance, and promote a more harmonised application of the GDPR across Member States.
	Development of Supplementary Implementation Guidance for Harmonised Application				
11.	**General Recommendation**	The draft template contains several legal and procedural concepts that are central to	The EDPB could accompany the final template with concise implementation guidance	The EDPB has consistently supported harmonised application of the GDPR	Accompanying the template with concise implementation

		the preparation of personal data breach notifications, including controller awareness, estimated dates, incomplete and follow-up notifications, and the assessment of risk and severity. While these concepts are reflected within the template, they are not consistently accompanied by explanatory guidance or practical examples.	containing explanatory notes and practical examples illustrating key concepts, including controller awareness, estimated dates, incomplete and follow-up notifications, severity assessment, and the application of conditional fields. Such guidance could be published separately from the template and updated periodically as supervisory practice develops.	through guidelines and practical implementation guidance. Providing concise explanatory material alongside the final notification template would promote a more consistent interpretation of key concepts, reduce uncertainty for controllers, and improve the quality and comparability of breach notifications without altering the template or imposing additional reporting obligations.	guidance would improve legal certainty, promote more consistent completion of breach notifications across Member States, reduce avoidable reporting errors, and support the harmonised application of Articles 33 and 34 GDPR.

CONCLUDING REMARKS

The Centre for Law and Technology, Faculty of Law, SRM University Delhi-NCR, Sonipat, respectfully submits this Report for the consideration of the European Data Protection Board as part of the public consultation on the Draft Standard Application Form for Personal Data Breach Notification under Article 33 of the General Data Protection Regulation (GDPR).

The Centre places on record its appreciation for the consultative and collaborative approach adopted by the European Data Protection Board in inviting observations and recommendations from stakeholders on this important initiative. Such a participatory process reflects the EDPB's continuing commitment to promoting the consistent and harmonised application of the GDPR across the European Union through practical, transparent, and effective regulatory guidance.

The Centre is of the considered view that the observations and recommendations contained in this Report are intended to further strengthen the Draft Template by enhancing legal clarity, promoting greater consistency in breach notification practices, and supporting the practical implementation of Articles 33 and 34 GDPR. The recommendations do not seek to alter the substantive obligations established under the GDPR but rather to facilitate their more consistent application through targeted explanatory guidance and contextual clarification. It is respectfully submitted that these recommendations may merit consideration while finalising the Draft Template, with a view to improving its usability, strengthening legal certainty, facilitating more effective supervisory assessment, and promoting a harmonised approach to personal data breach notification across the European Union.

The Centre remains committed to advancing research and contributing to evidence-based public policy at the intersection of law, technology, and digital governance. It is hoped that the observations and recommendations presented in this Report will constructively assist the European Data Protection Board in finalising a practical, coherent, and future-ready Standard Application Form that supports the effective implementation of the GDPR while strengthening the protection of the rights and freedoms of natural persons.

FACULTY OF LAW

RESEARCH TEAM AND CONTRIBUTORS



Prof. (Dr.) Paramjit Singh Jaswal

B.Sc., B.L. (Gold Medalist), LL.B., LL.M. (Gold Medalist), Ph.D., P.D.F. (London), Fulbright Scholar
Former Vice-Chancellor of the *Hidayatullah National Law University, Raipur, Chhattisgarh, India, Rajiv Gandhi National University of Law, Punjab, India and SRM University Delhi-NCR, Sonepat, Haryana, India*
Principal Advisor to the Chairperson, SRM Group.



Prof. (Dr.) Vijay Kumar Singh

Professor and Dean
Faculty of Law, SRM University Delhi-NCR, Sonipat, Haryana
Director, *Centre for Law and Technology, Faculty of Law, SRM University Delhi-NCR, Sonipat, Haryana.*



Dr. Shalini Saxena

Head of Department and Associate Professor
Faculty of Law, SRM University Delhi-NCR, Sonepat, Haryana, India
Member, Sub-Committee of the *23rd Law Commission of India.*



Dr. Shubham Singh Bagla

Assistant Professor
Faculty of Law, SRM University Delhi-NCR, Sonepat, Haryana, India
Faculty Coordinator, *Centre for Law and Technology, Faculty of Law, SRM University Delhi-NCR, Sonipat, Haryana.*



Dr. Jitendra Kumar Gautam

Assistant Professor
Faculty of Law, SRM University Delhi-NCR, Sonepat, Haryana, India
Faculty Member, *Centre for Law and Technology, Faculty of Law, SRM University Delhi-NCR, Sonipat, Haryana.*



Ms. Ruhani

Advocate and Legal Researcher
Alumna, *Faculty of Law, SRM University Delhi-NCR, Sonipat, Haryana, India*
Researcher, *Centre for Law & Technology, Faculty of Law, SRM University Delhi-NCR, Sonipat, Haryana, India.*

FACULTY OF LAW



Ms. Raka Medhavi

Assistant Professor
Faculty of Law, SRM University Delhi-NCR, Sonepat, Haryana, India
Faculty Member, *Centre for Law and Technology, Faculty of Law, SRM University Delhi-NCR, Sonipat, Haryana.*



Ms. Tahoora Kausar Syeda

Computer Science Student, University College of Engineering, Science and Technology Hyderabad (UCESTH), Jawaharlal Nehru Technological University Hyderabad
Intern, *Centre for Law and Technology, Faculty of Law, SRM University Delhi-NCR, Sonipat, Haryana*



Mr. Krishraj Singh Sikarwar

Law Student, Navrachana University, Vadodara
Intern, *Centre for Law and Technology, Faculty of Law, SRM University Delhi-NCR, Sonipat, Haryana*