VON WOBESER

E S G A R T I C L E S

Privacy and the protection of personal data: new ESG parameters

By: Luis Burgueño, *Partner*
Gloria Martínez, *Counsel*
Rubén Villegas, *Associate*

Recent decades have featured unprecedented growth and change across industries and the economy. New ways to do and fund business are rising with ever-greater speed thanks to globalization and new technologies. Hand in hand with these recent developments, awareness and concern about the side effects that both companies' and consumers' actions have on a global scale have increased, stressing newly found concerns for the well-being of both society at large and the environment.

Currently, customers and investors alike focus on more than financials when selecting new service providers and business opportunities, and those same providers and business partners must prove that their products and services surpass those of their competitors regarding sustainability, which comprises environmental, social, and governance (ESG) concerns. While the great majority of consumers already prefer companies that promote individual and collective welfare,[1] investors are also increasingly betting on companies that follow ESG criteria, interpreting them as a way to measure their susceptibility to both legal and reputational contingencies.[2]

ESG comprises a wide range of topics and activities inside three basic themes. However, all ESG criteria share the same focus: the impact companies have not only on their shareholders' interests, but also on those of customers and other stakeholders, considering aspects that go beyond the realm of mere compliance. Therefore, ESG should not be understood as a group of static or strictly legal goals or activities, but rather include new parameters and reportable criteria which should evolve along with those interests most valuable to a given society.

Accordingly, ESG criteria consistent with the modern world should include a new parameter: ensuring respect for privacy and the protection of personal data.

1 *Beyond Compliance: consumers and employees want business to do more on ESG*, PwC Consumer intelligence Series, accessed on June 2, 2021, available at: https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/consumer-and-employee-esg-expectations.html

2 Amir Amel-Zadeh and George Serafeim, *Why and How Investors Use ESG Information: Evidence from a Global Survey*, Harvard Business School Working Paper, No. 17-079, February 2017, available at: http://nrs.harvard.edu/urn-3:HUL.InstRepos:30838135

While ESG emerged in an economy rooted in fossil fuel-based industry and commerce, the present and future are led by digital rather than brick-and-mortar business models, and feature an economy built on the exchange and analysis of information. Bearing in mind that certain authors have called data the "new oil" of this new knowledge-based economy, the ESG focus -which seeks social commitment and welfare- should consider data protection as a key topic. Under what ESG heading could the protection of this data fall, and in what way could it be exercised inside the framework of law and everyday life?

The most widely used ESG reporting standards have included privacy and data protection under the "social" criteria group. Such classification would be justified by the fact that, due to the close relationship between personal data and access to financial services, telecommunications, transportation, and medicine, the breach of a single database could have devastating effects on entire communities. The same would be true for the company administering such a database, since it would have immediate exposure to both individual and class claims, as well as (harder to calculate) reputational damage. In a knowledge-based economy, any company without a clear strategy and awareness of the value placed on personal data would be ill-equipped to deal with the public and commercial consequences that come with an improper processing or breach of the same. This is yet another reason why data protection is a social concept with extralegal implications: it affects companies as much as their stakeholders, not just in terms of money but by affecting their private lives.

The social relevance of privacy and data protection already figures prominently in Mexico's legal system. The Mexican constitution considers both privacy and the protection of personal data as actionable human rights and provides for an independent regulator charged with their protection. Various federal and state laws oblige both public and private sector parties with informing data owners -individuals whose personal data is processed by a third party- of the terms of such processing, as well as requiring prior and informed consent for processing activities in general and immediate notice of any data breaches which may affect the relevant data owners. Such laws embody the social aspects of ESG in that they require data controllers to respect the principles of "loyalty and responsibility" toward data owners.

The "governance" aspect of ESG is also relevant when dealing with personal data protection and privacy. In order for the social commitments made by a corporate data controller to be effective, the security and vigilance of personal data processing as addressed by relevant legal provisions must be brought into companies' ordinary course of business, rather than being limited to the mere drafting of privacy notices or internal documents. In other words, formal measures must be made effective by an actual individual or department within the company that is sufficiently trained and empowered to ensure the due processing of personal data in tandem with other company targets.

While current Mexican legal provisions to such effect are limited, solely requiring the appointment of a person in charge of responding to data owner inquiries, the measures already employed by various companies, either based on foreign laws or on their own initiative, are good examples of the growing importance and link between ESG reporting and the protection of personal data. The appointment of C-suite officers specifically responsible for privacy compliance; the publication of internal procedures and policies intended to prepare company personnel for correct and minimal data processing within companies' production lines; and the hiring of consultants and third-party providers specialized in data security, are all examples of the same.

Considering the abundance of measures and stakeholders involved in the personal data ecosystem, it is evident why data protection generates concern. Although this protection is relatively new within the concept of ESG, the safeguarding of customer, supplier and investor information has had to be integrated suddenly in companies, since several organizations have experienced negative effects for not addressing this issue, which are manifested in the well-known personal data breaches.

The direct monetary cost incurred by North American companies for a given data breach

currently averages between 3 and 7 million dollars in the short term.[3] However, the damages derived from some of the most well-publicized breaches in recent times, including those affecting blue-chip players like Equifax, Facebook, Target, or Marriot, much like the ESG criteria, span many kinds of stakeholders and are multidisciplinary. They include class actions, government sanctions, damage both to companies' public standing and to their customers, which can be hard, if not impossible, to quantify. Moreover, the public has become increasingly wary of the value and dangers inherent to the processing of their personal data, as shown by the widespread resistance to recent legal initiatives designed to allow certain Mexican financial service providers and government authorities to process biometric data and contact information *en masse*.

Taking the above into account, it should be clear why any business should focus on personal data risk mitigation, and why both executives and investors alike would do well to promote it, even if it implies going further than mere compliance. Similarly, in a context such as the one we are currently living in, it is easy not only to explain the emergence of privacy and personal data protection criteria within the ESG accountability scheme, but also to predict that these matters will soon occupy a central place in the planning and life of companies. The only question remaining is: is your company ready?

3 John Zorabedian, *What's New in the 2021 Cost of a Data Breach Report,* July 28, 2021, available at: https://securityintelligence.com/posts/whats-new-2021-cost-of-a-data-breach-report/

For additional information, please contact our experts:

Luis Burgueño, Partner:
+52 (55) 5258-1003
lburgueno@vwys.com.mx

Gloria Martínez, Counsel:
+52 (55) 5258-1016
gmartinez@vwys.com.mx

Rubén Villegas, Associate:
+52 (55) 5258-1003
rvillegas@vwys.com.mx

VON WOBESER Y SIERRA, S.C.
Mexico City, November 17, 2021.