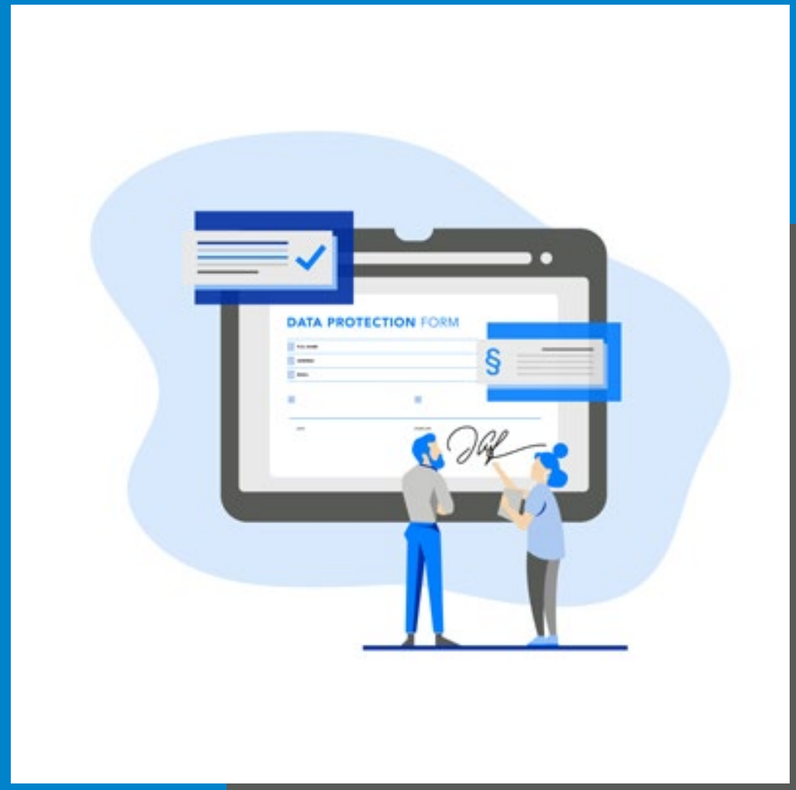
White Paper

Nacho Alamillo

GDPR and handwritten eSignatures

The new solution provider opportunity



wacom® for Business

GDPR and handwritten eSignatures

The new solution provider opportunity

Executive Summary: The EU's General Data Protection Regulation (GDPR) has created a new need to capture consent for data management purposes. Many organizations, especially those in financial services, healthcare and the public sector, are still capturing this consent in person and on paper – which is expensive, time-consuming and creates a workflow disconnect in this era of process digitization.

This reality makes GDPR a significant business opportunity for digital workflow solution providers serving organizations that rely on in-person transactions and/or consent capture. Although there are multiple ways to capture GDPR consent digitally, handwritten eSignatures are the most intuitive way for people to provide legally-binding and GDPR-compliant consent in person.

This report describes the GDPR business opportunity for digital workflow solution providers within the context of the legal status of handwritten eSignatures in the EU. It also defines the signature capture best practices that solution providers should follow to maximize this opportunity, while reducing risk for their customers.

GDPR compliance is a business critical issue → Compliance requires a documented signature workflow → GDPR consent capture is currently 95% paper-based →

Huge potential for workflow digitization!

Business process *optimization*

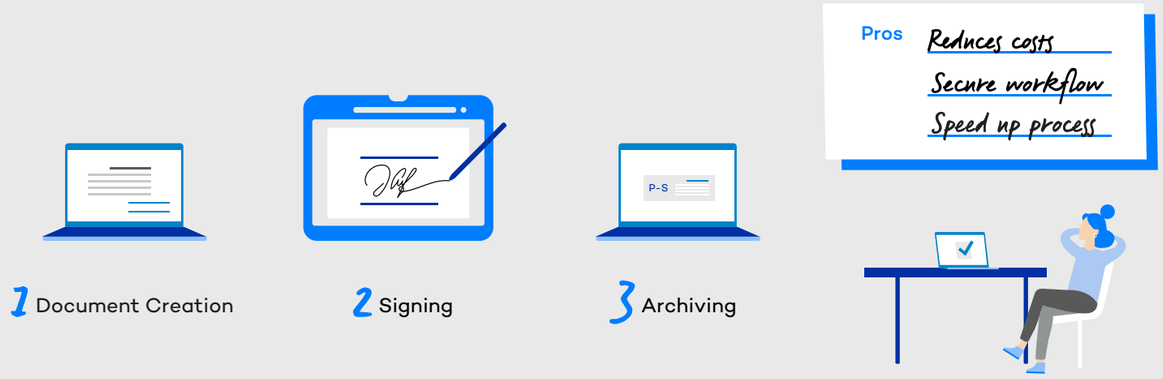
Why is GDPR a business opportunity for digital workflow and solution providers?

To comply with the EU's General Data Protection Regulation (GDPR), organizations of all kinds need to secure explicit consent from their customers to collect, process and store personal data. This requirement covers use cases as diverse as bank account applications, loyalty card sign up, consumer credit agreements, warranty claims, medical treatment consent and many more. GDPR covers methods of consent provision, such as handwritten signatures, as well as the personal data itself.

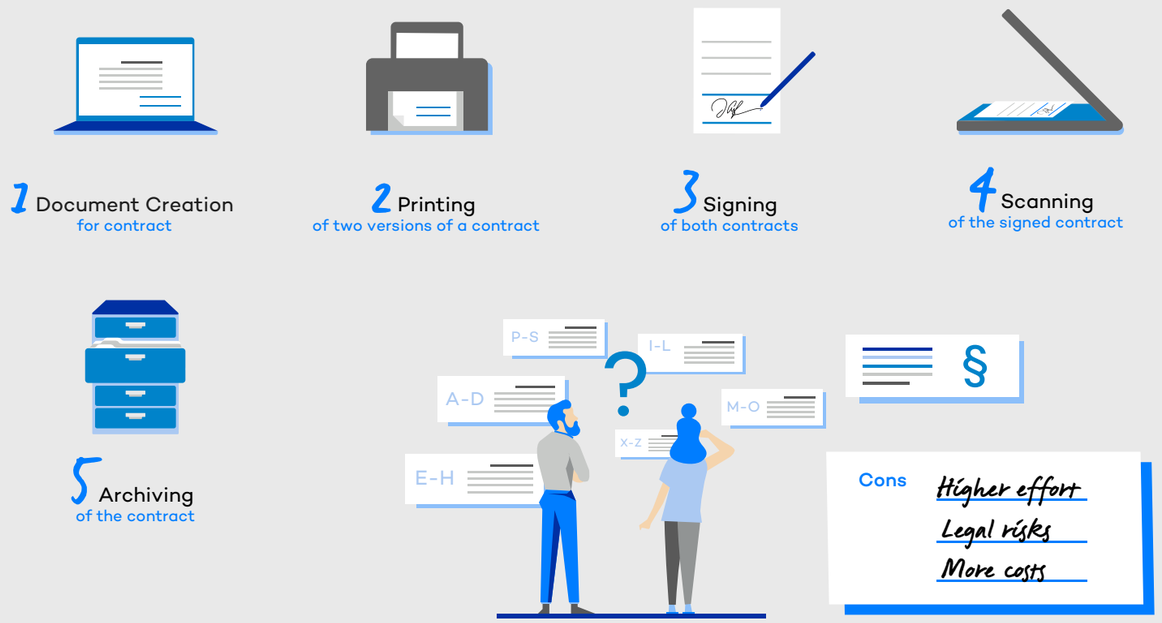
In the first few years of the GDPR era, consent has often been collected "in person" via traditional "wet ink" signatures using pen and paper – that is, the signature is created by the signatory in the physical presence of the party requiring the signature. Administratively, this is extremely inefficient and expensive, because paper forms need to be manually created, printed, collected, copied, scanned and archived, physically and digitally. Moreover, a paper-based approach is completely at odds with the drive to streamline, eliminate or digitize paper-based processes that most organizations are pursuing.

Nevertheless, handwritten signatures provided in person remain the most intuitive and legally valid way for people to provide their consent. That's why the closest digital equivalent – handwritten eSignatures – are the most effective way of digitizing the in-person GDPR consent process.

Digital GDPR consent workflow



Paper-based GDPR consent workflow



GDPR consent *A definition*

"Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."

Why are handwritten eSignatures the best choice for in-person GDPR consent processes?

1 **Convenient provision of explicit consent:** Handwritten eSignatures are the most intuitive and human way of providing GDPR consent, so that it can be easily integrated into digital workflows.

2 **Risk avoidance:** Using handwritten eSignatures to capture GDPR consent gives organizations a simple and relatively inexpensive way of minimizing the financial risk associated with non-compliance. Fines of up to 20 million EUR, or 4% of the global annual turnover of the preceding financial year can be applied, whichever is higher.

3 **Legal validity:** Handwritten eSignatures can provide an extra layer of validity, compared with pictures of signatures or checkboxes. The physical nature of the process makes signatures more intentional, the validity of which can be supported by the biometric data captured within a handwritten eSignature.

What is the legal status of *handwritten eSignatures in the EU?*

Handwritten eSignatures are admissible in court in any EU Member state, regardless of the technology used to capture them. Handwritten eSignatures created using digital devices are generally considered as Simple Electronic Signatures (SES), as explained in the info boxes on the next page. Theoretically, they could also be classified as Advanced Electronic Signatures (AES). However, since the fulfilment of AES requirements is open to interpretation and therefore legal challenge, this is not usually the case in reality.

eSignatures *Legal definitions*

In 2014, the EU introduced the Electronic Identification, Authentication and Trust Services (eIDAS) regulation. It is designed to enhance trust in electronic transactions between consumers, businesses and public sector organizations across the EU by establishing an assurance of consent validity. This covers all methods of providing consent electronically including checkboxes, handwritten signatures, etc., regardless of the technology used. eIDAS recognizes three ways of providing consent assurance:

Simple electronic signatures (SES): This could be a click in a box on a web form, or the capture of a handwritten eSignature on an electronic form on a digital device. The link to the signatory can be guaranteed by applying additional measures, and any suitable technology can be used.

Qualified electronic signatures (QES): The signature data is created by a Qualified Digital Signature Creation Device (QDSC), enabled with secure cryptography and validated by a certificate issued by a qualified EU Trust Service Provider (TSP). These stipulations make forgery extremely difficult. For this reason, a Qualified eSignature has direct full legal equivalence to an ink signature.

Advanced electronic signatures (AES):
A signature that creates data which can be uniquely linked to the signatory, that identifies him or her with a high level of confidence, and the alteration of which can be detected.

Digital signature
Electronic signature

Digital signatures vs electronic signatures

A digital signature is always protected by cryptography, whether it relates to a handwritten signature or some other form of consent provision, such as a fingerprint. Once the signature has been provided, neither it nor the document can be altered.

An electronic signature (eSignature) is not necessarily protected in this way, and could be provided in the form of, for example, an image of a signature pasted into a document. In this case, there is no guarantee that the consent is valid and has not been altered after the fact.

As such, a digital signature can be an electronic signature, but an electronic signature is not a digital signature if it is not cryptographically protected.

When is a handwritten eSignature GDPR compliant?

Because the creation of biometric data is intrinsic to the capture of a handwritten eSignature, absolute precision is required when determining when such a signature, used for capturing consent, is GDPR-compliant, and when it is not. This can be determined as follows:

Handwritten eSignatures are GDPR biometrics compliant:

If the biometric data associated with a specific handwritten eSignature is ONLY captured and stored (e.g. enciphered) and NOT processed through a specific technical means allowing the unique identification or authentication of a natural person, it is not considered as a biometric treatment under GDPR.

In other words, handwritten eSignatures can be used to capture consent without being affected by the strict provisions set forth in GDPR for biometric data, as long as they are not processed as described above.

Handwritten eSignatures may NOT be compliant with GDPR biometrics requirements: If the biometric data associated with a specific handwritten electronic signature IS processed for the purpose of uniquely identifying a natural person (e.g. comparing different signatures to assure the identity of the data subject) without a specific legal basis. In this case, the signature MAY BE subject to challenge under GDPR.

What are the best practices for ensuring GDPR compliance when enabling handwritten eSignatures for consent capture?

As described above, as soon as the biometric data contained within a handwritten eSignature is processed in a way which could uniquely identify the signatory, it's use may be open to challenge under GDPR's strict biometric data rules. This is due to the special sensitivity of biometric information in electronic form, as opposed to paper form.

This is why it's important to follow some specific guidelines when capturing handwritten eSignatures, in order to maximize their legal validity, while simultaneously minimizing the risk of GDPR non-compliance.

Best practices

1. **Use high quality handwritten eSignature hardware:** Ensure that the hardware used captures a broad range of biometric data that is recoverable in its raw form – not just in the form of a graphical representation.

2. **Ensure the signatory signs in an ergonomically optimized way**: i.e. seated, using the signing device on a desk, not crouching with no physical support for the tablet. Defective signature capture that, for example, leaves voids in the captured data or exceeds the physical border of the signature area, may invalidate the eSignature from a legal perspective.

3. **Ensure the captured signature is linked in a unique way to the purpose or meaning of the signature:** This ensures the eSignature and the document can, if necessary, be connected to an identifiable person. It must also be impossible for the signature to be linked to other content.

4. **Prove the organization capturing the eSignature cannot access or alter the data:** This can be achieved by storing a cryptographic hash of the signed document together with the eSignature data, and by using a trusted third-party acting by interposition to capture and store the data, and securely hold the encryption key. The captured signature data should also include an electronic timestamp to prove it has not been altered since it was created. A qualified electronic seal could be added to this data to add an extra layer of redundancy.

Best practices

5. **Define eSignature data retention periods and archival requirements:** This includes the technological specs for the systems used to store the data.

6. **Define comprehensive security rules and procedures:** Specifically, ensure the management of the encryption/decryption keys for the biometric data associated with a specific handwritten eSignature are defined and adhered to.

7. **Only use high quality, tested encryption keys:** It must be possible to prove that nobody has been able to access to the decryption key, and that backup processes have been established to prevent the loss of the decryption key. Regular key rotation (the periodic replacement of an existing key with a new one) can help reinforce proof of data integrity.

8. **Protect against risks created by third-parties:** Especially when a third-party is used to capture and store handwritten eSignature data, procedures must be in place to ensure that the data can be retrieved quickly enough if it is needed for a legal case. This must go beyond the provision of the decryption key to the organization requiring the eSignature, because this would destroy its legal validity i.e. the organization would be able to use the key to alter or misuse the data. There must also be procedures in place for the management and recovery of the data if the third-party no longer exists.

9. **Establish guidelines for the production of the evidence for legal proceedings:** It's essential to ensure that a legal report and a forensic computer report explaining the validity of the handwritten eSignature capture process are available quickly.

Conclusion
GDPR opportunity

Handwritten eSignatures that capture biometric data are a valuable, user-friendly way of capturing legally valid proof of consent in-person (for GDPR or other purposes), in a way that minimizes the risks associated with GDPR non-compliance.

It is also relatively easy to ensure handwritten eSignature capture does not conflict with GDPR requirements for biometric data treatment: Simply collect and store the handwritten eSignature data, without processing it in a way that could be used to uniquely identify an individual.

The exception to this is if you are required to do so in relation to a legal procedure, where the eSignature is being challenged by the signatory. At this point, you'll benefit from a legal basis within GDPR that allows you to defend your position. This includes the possibility, under a court procedure, to capture new samples of biometric eSignatures to compare the original eSignature, which will uniquely identify the signatory. While this does count as a biometric data treatment under GDPR, it is fully legal and compliant, because it is being performed in the context of a legal action.

Following the best practices outlined in this report will help ensure the legal validity of handwritten eSignatures should a court action require them to be used in evidence.

For this reason, rather than being a challenge to be feared, GDPR provides digital workflow solution providers with a significant new business opportunity in the form of enabling in-person handwritten eSignatures for capturing consent in a legally valid and GDPR-compliant manner.

Nacho Alamillo
Doctor in Law

About the author
Nacho Alamillo

Nacho Alamillo is Doctor in Law (UMU). He holds a Degree in Law (UNED), a Diploma of Advanced Studies (UAB) and a Master in introduction to administrative law research (UAB). He is also a Certified Information Systems Auditor, CISA (ISACA), a Certified Information Security Manager, CISM (ISACA), and is also certified in COBIT5 Foundations (APMG) and in ITIL V3 Foundations (EXIN).

Currently, he is a practising lawyer at Reus Bar, Managing Partner at Astrea La Infopista Jurídica SL, CISO at Logalty Servicios de Tercero de Confianza SL and an external researcher at iDerTec (University of Murcia).

He has authored/co-authored more than 80 publications and has delivered more than 400 conferences and courses relating to electronic identity, trust services and their application to electronic processes.

More Information:

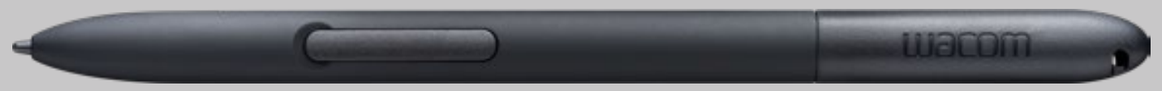
Wacom for Business is the global market leader in handwritten eSignature hardware and software. To discuss how to use our technology for your next in-person GDPR consent workflow project, please contact Wacom sales at:

solution@wacom.eu

For specific legal advice about eSignatures in relation to all forms of consent provision, please contact Nacho Alamillo Domingo at:

nacho@astrea.cat

More human



More digital

Japan (HQ)
For more information please contact:
Wacom Co., Ltd. · Sumitomo Fudosan Shinjuku Grand Tower 31F, 35F,
8-17-1 Nishi-Shinjuku, Shinjuku-ku, Tokyo 160-6131, Japan
vm-info@wacom.co.jp · 03-5337-6706

Americas
For more information please contact / Pour de plus amples informations, veuillez contacte / Para obtener información adicional, póngase en contacto con: Wacom Technology Corporation · 1455 NW Irving Street, Suite 800 | Portland, OR 97209 USA
esign@wacom.com · 1-503-525-3100

Europe, Middle East and Africa
For more information please contact / Pour de plus amples informations, veuillez contacte / Para obtener información adicional, póngase en contacto con: Wacom Europe GmbH ·Völklinger Straße 1, 40219 Düsseldorf, Germany
solutions@wacom.eu · +49 211 385 48 0

wacom® for Business

China
For more information please contact:
Wacom China Corporation · 518, West Wing Office, China World Trade Center, No. 1 Jianguomenwai Avenue, Chaoyang District, Beijing 100004, China
e-signature@wacom.com · 400-810-5460

Hong Kong
For more information please contact:
Wacom Hong Kong Ltd. · Unit 1610, 16/F, Exchange Tower, 33 Wang Chiu Road Kowloon Bay, Hong Kong
e-signature@wacom.com · +852 2573 9322

Australia
For more information please contact:
Wacom Australia Pty. Ltd. · Ground floor, Building 1, 3 Richardson Place, North Ryde, NSW, 2113, Australia
Contactapbs@Wacom.com · +61 2 9422 6730

Korea
For more information please contact:
Wacom Korea Co., Ltd. · Rm #1211, 12F, KGIT Sangam Center, 402 Worldcup Bukro, Mapo-gu, Seoul 03925, Korea
Contactapbs@Wacom.com · 080-800-1231

Singapore
For more information please contact:
Wacom Singapore Pte. Ltd. · 5 Temasek Boulevard, #12-09, Suntec Tower Five, Singapore 038985, Contactapbs@Wacom.com · (503) 525-3100

India
For more information please contact:
Wacom India Pvt. Ltd. · 426, Tower B, DLF Building Jasola District Centre, Mathura Road, New Delhi 110025 India, Contactapbs@Wacom.com
Customer Support: 000-800-100-4159, +91-11-47239412

wacom.com/for-business