

datum : Kies een datum.
onze referentie : Geef onze referentie.
uw referentie : Geef referentie geadresseerde.
onderwerp : Implementation of new privacy legislation (GDPR) at VIVAT

Burg. Rijnderslaan 7
Postbus 5000
1180 KA Amstelveen
www.zwitserven.nl

T.
E.

Dear Sir, Madam

It has increasingly been a topic of conversation over the last few weeks. 25 May 2018 will see the introduction of new EU privacy legislation on how companies are to deal with personal data, of customers as well as staff. It is a good time to let you know what the new privacy rules mean for us and how we will be handling (your) personal data, what we are doing to put the new rules into effect, and what you can expect from us over these coming months.

Zwitserven – VIVAT

Zwitserven is part of the VIVAT group; it is a 100% subsidiary of VIVAT N.V.
Based on inter-company arrangements, VIVAT N.V. is responsible for handling personal data for all companies within the VIVAT groep.

Where we are with the introduction

The arrival of the new privacy rules does not only mean that we have to implement new processes and adjust our systems. We are also working hard to inform and train all our staff, and have appointed a Data Protection Officer and Privacy Officers. They know all about the new privacy legislation and are responsible for monitoring compliance with the new rules. The Privacy Officers are also the first port of call for our staff if they have a privacy-related question.

Risk-based approach

The measures that we are putting in place to implement the new legislation are all consistent with the purpose of the new legislation, which is to handle the personal data of our customers and staff with due care. We have chosen a risk-based approach. This means that we are taking extra measures if there is a higher risk, for example where medical details or data on criminal convictions and offences are concerned. Similarly, additional measures will be put in place for financial data and Citizen Service Numbers (BSNs) so as to ensure that these data are extra protected.

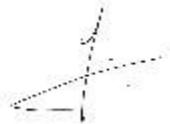
VIVAT's privacy principles

On the next page, you will see a summary of the most important changes for us and "VIVAT's 10 Privacy Principles". In the run-up to 25 May, we will regularly keep you up to date on these changes and our activities in terms of implementing the new privacy legislation.

Any questions?

If you have any questions about this letter, please contact your adviser. Alternatively, you can call «Naam_IAM» on «Telnr_IAM» or send an e-mail to «Email_IAM»

Kind regards,



Hans Visser
General Manager

VIVAT's 10 Privacy Principles

1. We will access and process personal data only if necessary to achieve a specific and predefined purpose.
2. In no event will we process more personal data than is necessary or hold personal data for any longer than necessary.
3. Everyone within the company is personally responsible for the careful handling and security of personal data in accordance with our Privacy Risk Policy and specific privacy policy documents and guidelines.
4. We will work continuously to raise privacy awareness among our employees by providing training courses and awareness materials, and through the Data Protection Officer and Privacy Officers in case of privacy-related questions.
5. All security incidents involving or likely to involve personal data will be reported to the Incident Reporting Desk immediately after discovery.
6. We are open about how we process personal data and about the rights that data subjects can exercise.
7. Our customers will have control of their personal data.
8. Each time we process high-risk personal data, we will conduct a Data Protection Impact Assessment (DPIA) to identify privacy risks and take appropriate measures.
9. Before processing, we will ask customers for their unambiguous consent if we have no other legal basis for the data processing.
10. We operate a uniform privacy approach across the company (for all productlines)

Most important changes GDPR



Accountability. VIVAT must Be able to demonstrate Compliance with the GDPR:
(i) maintain a **record of processing activities**
(ii) conduct a data protection **impact assessment** for more risky processing



Profiling will require a legal basis (consent) and customers have the right to opt out



VIVAT should be able to demonstrate that **customers understand the intended use of their data.** All privacy notices in clear & plain language



Customers have the right to rectify and remove data that is being held without legitimate reasons, including the right to be forgotten



Customers have the right to obtain a copy of their personal data from VIVAT in a standard portable format and have this transferred to another company



Obtaining **consent** for processing personal data must be **freely given, specific, informed and easy to withdraw.** VIVAT must be able to demonstrate that consent was given



Non-EU business will be subject to GDPR if they offer goods or services to EU residents



Data breaches must be notified to the regulator (AP) **within 72 hours** after having become aware of it. Data processors must notify VIVAT of a breach without undue delay



Privacy by Design & by default
Products should be sourced and designed with privacy in mind
Most friendly privacy option is the default setting



Data Protection Officer
Obligatory if activities involve large scale or systematic monitoring of sensitive personal data
Independent role with a focus on advising controllers and monitoring compliance



Maximum fines of € 20 M or 4% of annual worldwide turnover