FE - Introduction

With the PAYONE Frontend hosted-iFrame you have a compliant solution even with using external references (e.g. images, self-hosted CSS) and customized JavaScript. The basic requirements to be eligible with SAQ A Please refer to PCI DSS Security Standards listed in SAQ A V3 on https://de.pcisecuritystandards.org are:

- Your company accepts only card-not-present (e-commerce or mail/telephone-order) transactions;
- All payment acceptance and processing are entirely outsourced to PCI DSS validated third-party service providers;
- Your company has no direct control of the manner in which cardholder data is captured, processed, transmitted, or stored;
- Your company does not electronically store, process, or transmit any cardholder data on your systems or premises, but relies entirely on a third party(s) to handle all these functions;
- Your company has confirmed that all third party(s) handling acceptance, storage, processing, and/or transmission of cardholder data are PCI DSS compliant; and
- Your company retains only paper reports or receipts with cardholder data, and these documents are not received electronically.

and

- The entirety of all payment pages delivered to the consumer's browser originates directly from a third-party PCI DSS validated service provider(s).

PAYONE provides now the PAYONE Frontend hosted iFrame for input of sensible credit card data which is fully PCI DSS 3.1 SAQ A compliant.
Therefore a new URL has to be used: **https://frontend.pay1.de/frontend/v2/**.
For security reasons the new PAYONE Frontend hosted-iFrame

- does not populate credit card details with given data.
- must not be used with option "autosubmit=yes" and credit card data.
- has to be hosted on new domain and URL **https://frontend.pay1.de/frontend/v2/**