DMARC at Krones

If you wish to secure e-mail communication between you and Krones (item 3.) please read this document carefully.

1. Why is Krones introducing DMARC?

Using DMARC (Domain-based Message Authentication, Reporting and Conformance; RFC 7489), Krones will enable its e-mail communication partners to verify the authenticity of an e-mail message from the Krones Group at the beginning of 2023.

2. How does DMARC work? (Information for IT staff)

DMARC improves/combines the protection functions of two well-known procedures:

SPF (Sender Policy Framework):

- Checks whether the IP address used for sending is released/authorised for this purpose by the domain owner.

DKIM (DomainKeys Identified Mail):

- The mail server adds a digital signature to the e-mail when it is sent.
- Signature is matched with the public key in the DNS zone of the domain

The DMARC check is successful if:

a. the SPF check of the sender's IP address is successful **and** the FROM header from the RFC-5322 Message Header matches that of the RFC-5321 field. Or:

b. the DKIM digital signature was successfully verified **and** the signature domain matches the domain from the FROM field of the RFC-5322 Message Header. Or:

c. both a and b are fulfilled.

Krones will use the DMARC policy **Reject** from the beginning of 2023.

3. Securing e-mail communication between you and Krones

Each recipient should configure their e-mail server to perform a DMARC check on each incoming email and either reject or quarantine non-compliant emails.

If the DMARC check is not activated on the recipient's side, the recipient will not be able to benefit from the Krones Group's advanced security measures but will not otherwise experience any technical restrictions.

Furthermore, we recommend that all Krones communication partners also secure their own email communication using DMARC.