


## Tyrol Military Command Protects Citizens' Protected Health Information During Global Health Crisis

**OVERVIEW**



**Customer:** Austrian Federal Army  
**Partner:** Ontrex AG, CH  
**Industry:** Government  
**Location:** Tyrol, Austria

**Kiteworks Capabilities Used:**

- Email
- File Transfer
- Automated File Transfer
- File Sharing
- APIs
- Web Forms

The Austrian Federal Army provides not only core defense services but also assistance to the Republic of Austria in the event of natural disasters. The Army, for example, performed a variety of tasks in the early weeks of the coronavirus pandemic.

Soldiers of the Tyrol Military Command were stationed at border crossings and tasked with checking entry and exit documents, collecting health data, and taking motorists' temperatures to monitor for fevers. The soldiers performed these tasks efficiently and effectively. The challenge was transmitting this data to the civilian authorities.

### Myriad Challenges Complicate Secure File Sharing

At the beginning of the mission, data was transmitted either manually or in hard copy. The army's IT systems were cumbersome and not user-friendly, and were simply unavailable to the soldiers deployed in the field.

The army therefore relied upon unsecure, consumer-grade solutions like email, Dropbox, and WhatsApp to transfer this sensitive data. The Tyrol Military Command needed a comprehensive and, above all, secure solution for sharing personally identifiable information (PII) and protected health information (PHI) with civilian authorities and their trusted partners.

In order to comply with the Federal Ministry for Digitalization and Economic Affairs' "Digital Team Austria" initiative, the file transfer solution must also improve cooperation between the Austrian Federal Army and "blue-light" organizations like the Red Cross, customs, police and fire brigades, and critical infrastructure organizations. Lastly, the solution must be easy to deploy and easy for everyone to use.

**“Thanks to the solution’s ease of use, for me as an administrator as well as for the users, it is fast and straightforward to set up and use—and that’s particularly important in crisis situations.”**

**– Administrator, Tyrol Military Command**

## Case Study

### Tyrol Military Command

## Security Is Paramount, But So Is Governance, Ease of Use, and Cost

Since the organizations involved had different focuses and IT technologies, linking the IT systems was neither expedient nor wanted, and for cost reasons it was not the desired solution.

It should be possible for both the permanent and ad hoc forces of the blue light organizations and the Austrian Federal Army to share information quickly, securely, and above all, in a user-friendly manner. In this context, secure means that the information is consistently protected in all phases and can neither be sent to third parties nor opened from the “outside” (i.e., decrypted). The IT system to be used should be intuitive, quick to learn, and largely oriented toward familiar functions of common IT applications to also minimize training time and costs.

## The Right Solution at the Right Time

The army first had to define its security requirements. The PII and PHI shared must be consistently protected in transit and at rest. Second, this information must not be transferable or viewable to unauthorized third parties. The army sought to adopt the “Zero-Trust Model,” based on the principle of not trusting any device, user, or service inside or outside one’s own network. This minimizes risks and eliminates potential threats.

Ontrex AG, one of the army’s strategic partners, identified Kiteworks as best suited to provide a timely proof of concept for the decision-makers at the Tyrol Military Command. This solution was deployed as Software-as-a-Service on a secure cloud instance allocated only for this application in the European AWS cloud. The system was rapidly implemented and ready for use for everyone involved after about 60 minutes of training.

Kiteworks was able to demonstrate compliance with the Tyrol Military Command’s requirements for confidentiality, integrity, and availability of information. Data confidentiality means that no unauthorized persons or organizations could read the transmitted and stored information. The integrity of the data ensures that the information remains unchanged (i.e., in the original) at every stage. And, of course, the data has to be available to the parties involved at any time.

With Kiteworks, sharing information between authorities and organizations is possible without having to integrate with or migrate to any one organization’s IT systems. Each endpoint device contains the latest or most current file version, and access is role-based and trackable. A unified, standardized reporting system ensures complete transparency throughout the entire data flow with trusted partners. As a result, the Tyrol Military Command now complies with legal regulations like GDPR as well as internal audits, policies, and procedures. Encrypted, state-of-the-art storage ensures maximum content security and prevents sensitive data from being transmitted to or read by unauthorized devices or persons.

Kiteworks is not only secure, it’s also easy to use. Sensitive data is located quickly and easily with a smartphone and sent securely and encrypted to the recipient.

## Needs

- Secure data transfer of civilians’ personally identifiable and protected health information between civilian authorities, organizations, and the army while protecting borders during COVID-19 mission
- Cross-organizational cooperation with changing teams (temporarily deployed soldiers and volunteers)

## Kiteworks Solutions

- Kiteworks Secure File Sharing for securely sending PII and PHI from the field to multiple organizations
- Kiteworks Secure Email for maximum, Zero Trust security that also demonstrates compliance with internal policies and data privacy regulations
- Kiteworks Secure File Transfer for secure, governable file exchange of sensitive information

## Business Impact

- Citizens’ personally identifiable and protected health information is protected in transit and at rest in compliance with GDPR to help monitor and contain COVID-19 transmission

## Case Study

### Tyrol Military Command

## Additional Use Cases

During its COVID-19 mission, the Tyrol Military Command identified other use cases for Kiteworks. Prior to deploying Kiteworks, it was a major challenge for blue-light organizations to convince their voluntary staff not to store or send sensitive data while on duty via unsecure cloud applications, such as Dropbox or WhatsApp, on their mobile phones. With Kiteworks, staff shares PII, PHI, and other sensitive data much more safely, and above all, without any training. The Tyrol Military Command had lots to worry about during its COVID-19 mission. Once they deployed Kiteworks, sharing sensitive content with trusted partners became one less problem to worry about.

**“The solution is exceptionally well-suited to civil/military use due to its maximum data security and complete traceability.”**

**– Administrator, Tyrol Military Command**

### Kiteworks Partner:

# Ontrex

Ontrex AG  
Haldenstrasse 23  
8306 Brüttisellen  
Switzerland  
Phone: +41 44 835 1000  
E-mail: [info@ontrex.ch](mailto:info@ontrex.ch)

Based on many years of experience and a highly qualified team, we ensure to keep up with the dynamics of the market and to react accordingly to customer needs. As a result, we support our customers not only by reducing IT costs and increasing system availability, but also by being able to act proactively and quickly to meet the needs of their business requirements.

The headquarters of Ontrex AG is located in Brüttisellen (CH); a branch office is in Munich (Germany). The team consists of over 40 employees. Ontrex serves over 400 customers.

# Kiteworks

Copyright © 2022 Kiteworks. Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and save of sensitive content. To this end, we created a platform that delivers content governance, compliance, and protection to customers. The platform unifies, tracks, controls, and secures sensitive content moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all sensitive content communications.