IPlytics Security

The security, privacy and anonymity of your data is vitally important to us. Therefore, IPlytics takes data security and the privacy of your personal and work-related information very seriously. Our software tool IPlytics Platform is built with industry-standard security procedures and employs strict policies to protect your information. As a German company IPlytics is subject by law to all national legal requirements of data security and privacy which belong to the strictest in the world.

as of January 2019

Product Security Features

ENCRYPTION	
Secure Authentication & Credential Storage	IPlytics follows secure credential storage best practices by never storing passwords in human readable format, and only as the result of a secure, salted, one-way hash. IPlytics guarantees an advanced password security relying on bcrypt as our core hashing algorithm with a per-user salt and multiple execution iterations of hashing to deter brute force attacks, making it computationally infeasible that your password could be recreated from the hashed form.
Data Encryption	IPlytics secures your information by encrypting it when it's sent over the Internet, storing it in an encrypted format when kept on a server. This means that your information is protected from unauthorized access not only when it's stored in IPlytics Platform but also while it is being transmitted to and from your devices (see network security). IPlytics will never provide information to third parties; this relates especially to sensitive search queries and reporting.

Data Center & Network Security

PHYSICAL SECURITY

Facilities	IPlytics servers are hosted at compliant facilities that meet rigorous security standards and undergo annual third-party audits of all management, hosting, network services, and operating procedures. Amongst the top certifications are ISO 27001, ISO 27018, SOC 1 Type 2, SOC 2 Type 2, CSA Start Level 1, EU Model Clauses.
Location	IPlytics keeps business as well as customer data in Germany, and the Netherlands, having datacenters in Frankfurt am Main and Amsterdam. While any customer-related, externally inserted data, is stored exclusively in Germany, only the internal default data of IPlytics Platform itself runs on servers in Amsterdam.
Monitoring	All systems, networked devices and circuits are constantly monitored by both IPlytics and our co-location providers.
On-Site Monitoring & Security	Our datacenters are physically constructed, managed and monitored 24/7/365 to shelter data and services from unauthorized access as well as environmental threats. Access to the IPlytics systems by authorized personnel only is strictly controlled via lock box processes, pass-cards and/or biometric finger scan units.

NETWORK SECURITY

Transmission Security	Communication between you and IPlytics Platform servers are encrypted via industry best-practices HTTPS and Transport Layer Security (TLS). This ensures that all traffic between you and IPlytics Platform is secure during transit. Communication is secured through AES and a SHA-256-algorithm with RSA-encryption to prevent an interception of sensitive data between your system and our servers. IPlytics encryption is provided by COMODO PositiveSSL with 4096-bit private key and SHA-2 signature algorithm.
Dedicated Security Team	Our Security Team is on call 24/7 to respond to security alerts and events.

On-Site Monitoring & Security (IDS/IPS)	Our network is protected by firewalls, secure HTTPS transport over public networks, regular audits, and network intrusion detection/prevention technologies (IDS/IPS) that monitor and block malicious traffic and network attacks.
Network Vulnerability Scanning	Network security gives us deep insight for quick identification of out-of-compliance or potentially vulnerable systems.
Third-Party Penetration Tests	In addition to our extensive internal scanning and testing program, each year IPlytics employs third-party security experts from Ifis (Institut for Internet Security, Westfälische Hochschule) to perform a broad penetration test across the IPlytics Platform network.
Logical Access	Access to the IPlytics Platform Production Network is restricted by an explicit need-to-know basis, utilizes least privilege, is frequently audited and monitored, and is controlled by our Operations Team. Employees accessing the IPlytics Platform Production Network are required to use multiple factors of authentication.
Security Incident Response	In case of a system alert, events are escalated to our 24/7 teams providing Operations, Network Engineering, and Security coverage. Employees are trained on security incident response processes, including communication channels and escalation paths.

AVAILABILITY & CONTINUITY

Disaster Recovery	Our disaster recovery program ensures that our services remain available or are easily recoverable in the case of a disaster. This is accomplished through building a robust technical environment, creating disaster recovery plans, and testing.