FILMATIC PRIVACY POLICY

The Privacy Policy of Filmatic Packaging Systems Pty Ltd explains how we as a group company obtain and use the personal information of individuals in the way that it meets the requirements of the Protection of Personal Information Act (POPIA).
Here at Filmatic, we can assure you that your personal information cannot be safer and more secured. This means that we are doing everything in our power to protect your privacy and that the information we collect amongst our people are used in a lawful and proper way which will not violate the POPIA Act.

Who we are:
Since our inception in 1979, our manufacturing facility has been located in Paarl, the middle of the Western Cape winelands district of South Africa. Filmatic is also part of the Trepko Group of companies. As one of South Africa's top packaging systems design and manufacturing companies, Filmatic supplies packaging equipment solutions that can accommodate packaging of all types of glass and plastic bottles, sachets, tubs, cups and literally most conceivable containers and closures. We provide our services to the dairy, cream, water, beer, fruit juice, jam, honey, shampoo, dish washing liquid, ketchup, vinegar, motor oil, edible oil, wine and cider production industries to name but a few.

Combining our own manufacturing of engineered designs through a team of highly skilled mechanical and electrical engineers and the equipment sourced from approved agencies around the world, we are able to provide the complete solution in packaging needs, including all operational aspects of a turnkey packaging line, which is supported by our 24-hour service stand-by commitment through highly skilled technicians and maintenance teams that provide comprehensive services to our clients worldwide.

Type of personal information we are collecting:

At the moment we obtained your personal Information in 2 ways namely, each day there will be a popup on our website where you will have the opportunity to insert your email if you want to be part of our newsletter which will be shared to our users each month. If you are not comfortable sharing your information you can just close the popup and it won't come up again for a whole day. Next, we have a contact us page where users can engage with us through email. There are different fields that needs to be filled in for example: Full name, Company Name, Email Address, Contact Number, where you are based, Type of enquiry, machine in question, message and also there is a multiple-choice question where you must decide if you are willing to receive company and product updates.

For what purpose are we using your personal information for?

After you filled in the contact form it will immediately be directed to the sales team at sales@filmatic.com where they will be taking care of you. We will therefore have access to all of the information provided to us by you in the contact form and that is just to help the sales team understand your enquiry and to help you immediately in the process. It is much easier to understand the request if the form is completed and nothing has been left out. We are also using your personal information for marketing purposes for detailed targeting such as email campaigns where we will share relevant information regarding our company, solutions, projects, machines etc. to you and promise not to bother you and spam you with lots of emails.

The following source allows us to receive personal information indirectly:
We make use of cookies which you can choose to accept or decline when visiting our website and if you choose to accept it, we collect internet (website) visitor usage information. This means that the information collected through website cookies will only be used for specific purposes what you agreed for.

How we store your personal Information:
IT Setup, Registers Documents control

- The network setup information, administrative accounts and passwords and essential security information is captured in the Filmatic Site document.
- All IT assets and the allocations thereof are recorded in the IT assets register and maintained by IT personal. • These are protected, controlled documents and stored in a secure network location and can only for used/accessed by the IT department and may not be distributed or made available to any party other than a company director.
- Personnel contact information is made available to network personnel by means of the e-mail system and a Filmatic contact list. This governed and controlled by the Filmatic IT Users policy.
- No personal information is recorded in the company's telephone system, other than a name and extension.

Archiving and Backups:
- All e-mails are internally backed up and externally archived.
- E-Mails are archived with a 1O+ year retention period.
- All on-premise digital data (network data) and network servers are replicated to the DR (Disaster and Recover) server room and backed up, by automated backup policies, to disk (internal storage) and then duplicated to data tape (removeable media). The removable tape media is moved to an undisclosed secure location. The retention periods are controlled by the backup policies. The retention periods for on-premise data are:
- The backup to tape retention periods for the various types of network backup policies are:
- Full Yearly backups to tape Backup solution lifetime
- Full Monthly backups to tape 5+ Years incremental backups to tape Next Full backup to tape+ o Differential backups to tape Next Differential backup to tape+
- The retrieval/restore of backups is limited to the IT department and is protected by a secure service and user account.

Data Protection Rights:

Security and Network access:
- Network security and access is controlled, with system security policies and enforced and monitored by the network system. This is achieved by means of user accounts with passwords with only allowed domain joined devices.
- These users and devices are protected thru:

o Anti-Virus agents that are deployed and centrally managed and monitored.

  - Firewall policies and rules that protect the network from external threads and also controls internal users' access to the internet. Remote access is protected and controlled by a firewall as well as a remote access server.

Only users in a security group are allow remote access.

o Access to removable storage (USB drives/External drives) on domain joined devices are controlled by system policies for selective groups to protect confidential company data from distribution.

- The network file-based storage on the company network file system is protected from malicious data files by:
  - FSRM (File System Resource Management) policies, which will prevent selectively certain file types in selective network locations. This will either warn the users or block the saving/storing of the file. This provides additional security against viruses, malicious software and against ransomware
  - All network server is protected by Anti-Virus agents that are deployed and centrally managed and monitored.
  - Encryption is not allowed on the company network system and blocked. This provides the network protection against "Ransomware" threads.

- **The company network server room:**

o The main server room is in a secure access-controlled location. The servers and services are in a redundant configuration, for protection of hardware failures.

o The DR (Disaster and Recover) server room is in a different secure, access-controlled, location. The DR servers are in a redundant hardware configuration, for protection of hardware failures.

o Only the IT department have access to the server rooms.